ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 02-26-2007 BY 60324 AUC BAW/CPB/STP

SECTION 2. FIELD OFFICE OPERATIONS

2-1 APPEARANCE AND MAINTENANCE OF OFFICES

2-1.1 Maintenance of Official and Personal Property (See Legal Attache Manual, 2-11 & 3-3.)

The SAC is responsible for the maintenance of the office in a neat and orderly manner and for the care of all property.

(1) Official papers, documents, books, and similar materials are not to be kept in desk drawers, but file cabinets for this purpose are to be supplied.

(2) Agents may keep in their desks: briefcases; bound Bureau bulletins; notebooks containing the most recent course of training received at the Bureau for 90 days (notes taken at specialized schools may be retained until separation from service); notes of annual and special conferences for 90 days; sidearm; not more than 50 rounds of ammunition for same; personally owned blackjack; current bound office memoranda; current diary; current National Academy Directory; office supplies for one week; map and street guide of the territory; copies of expense vouchers for one-year period; speech material of a current nature; latest issue of Bureau publications; dust cloth; and personal items currently used, segregated and neatly maintained, including smoking supplies, toilet articles in envelope or box marked personal, medicines, personal purchases made during the day, personal mail received during the day. Although employees are permitted to maintain certain personal belongings in their desks or other prescribed areas in FBI offices, no desk, drawer, cabinet, or any other space within FBI offices shall be considered to be the private space of any employee. (See Correspondence Guide-Field, 1-1(4) and Correspondence Guide-FBIHQ, 1-11.5.)

(3) Manuals, Bureau bulletins, SAC letters, Memoranda to all SACs, office rosters, and office telephone directories must be maintained in a safe and secure place so that they are not available to unauthorized individuals. (See MAOP, Part II, 2-1.3(5).)

2-1.2 Space Matters - Field Office

2-1.2.1 Repairs

(1) Minor repairs should be obtained through the building custodian.

(2) Major repairs must be authorized by FBIHQ.

2-1.2.2 Improvements and/or Structural Alterations

(1) Whether government or nongovernment building space, improvements and/or structural alterations must be authorized by FBIHQ. This is accomplished by executing a Reimbursable Work Authorization (RWA), General Services Administration (GSA) Form 2957, and submitting it to GSA. After GSA completes their portion of the form, it should be submitted to FBIHQ for approval with a letter of justification. A detailed cost breakdown of the work should be included in the cover letter. If approved, the form will then be returned to the appropriate field office for transmittal to GSA and subsequent commencement of the work.

(2) Annually, on a fiscal year basis, field offices may submit to FBIHQ, Attention: Space Management Unit, Facilities Management Section, Administrative Services Division, for approval an open-end RWA (GSA Form 2957) for an initial amount not to exceed $5,000. The open-end RWA is to be used for minor alterations and repairs to field office space. All other building space improvements and/or structural alterations must be requested separately and authorized by FBIHQ through the execution of GSA Form 2957 as set forth above.

Upon receipt of the approved open-end RWA, it should be submitted to GSA, thereby authorizing GSA to perform minor alterations and repairs to field office space when requested by the field office. The field office must maintain a log documenting the date, purpose, and cost of each obligation made against the open-end RWA. When the initial $5,000 has been depleted, requests for amendments to the initial RWA may be submitted to FBIHQ for approval in increments of $5,000 up to a total of $25,000 within a fiscal year for each field office. FBIHQ approval of amendments to the initial open-end RWA will be based on the justification submitted in support of the increase and the demonstration of responsible administration of the funds as evidenced by the logs.

(3) Annually on July 1, each field office holding an open-end RWA will be required to submit an amended RWA to FBIHQ returning the unused funds of the open-end RWA.

(4) For leased buildings where the field office representative has lease management authority, for alterations under $25,000, a scope of work for requested alterations must be developed, a government estimate obtained from the Planning, Design and Construction Management Unit, and bids obtained and submitted to the Space Management Unit (SMU) along with an FD-369 (Requisition for Services). (Note: If not within the field office authority to obtain bids, request will be forwarded to the Construction and Laboratory Contracts Unit (CLCU) to negotiate bids.) If approved, the request will be forwarded to the CLCU for the issuance of a purchase order. If the Administrative Officer has procurement authority, the requisition will be forwarded back to the field office for issuance of a purchase order. The Facilities Management Section will determine who the Contracting Officer's Representative will be for each alteration project request.

2-1.2.3 Space Requests

Requests for space and appropriate justification must be submitted to FBIHQ, Attention: Space Management Unit, Facilities Management Section (FMS), Administrative Services Division (ASD). If approved, the request for space will be submitted to the GSA by GSA Form SF-81 as prepared and submitted by the Section Chief, FMS, ASD. This procedure will ensure proper preparation of the request, that it is in compliance with existing Executive Orders and GSA and DOJ directives, and will also ensure space is acquired within funding levels set by Congress. Contacts or correspondence with GSA regional offices of other than a routine nature must be approved by FBIHQ. Any
requests to GSA concerning additional space, release of space, layout changes, renovations or any other changes in present or proposed field office space must be approved by FBIHQ prior to negotiations or commitments to GSA for such changes. Only GSA is authorized to conduct space surveys to locate space, and any activity by the Bureau in this area could result in inflated rental prices. If space suitable to your needs comes to your attention, there is no objection to advising

GSA of this fact, but surveys or checks with realtors should not be conducted. There is no objection to contacting local GSA representatives concerning day-to-day maintenance problems pertaining to space unless some particular reason exists for advising FBIHQ. Keep FBIHQ advised concerning local developments with GSA in space matters.

2-1.2.4 New Construction

Requests from GSA for office space requirements for proposed new Federal construction (GSA Form 144) must be forwarded to FBIHQ for handling.

2-1.2.5 Field Office and Resident Agency Relocation

Immediately following any field office or resident agency relocation, submit Form FD-607 (Field Office and Resident Agency Change in Address or Telephone Number) to FBIHQ advising effective date of occupancy change, street and mailing address, the telephone numbers and the date the Intrusion Detection System installation was completed. A copy of Form FD-607 should be marked to the attention of the Facilities Management Section, WB-950. Copies of the same communication should be forwarded to all other field offices. FBIHQ should also be advised when additional space is acquired or excess space is released. Submit this information to FBIHQ by electronic communication, Attention: Facilities Management Section. (See MAOP, Part 2, 1-3.7.)

2-1.2.6 Commercial Space

Communications favorably recommending acceptance of commercial space for FBI use must also indicate results of credit, arrest, indices, and pertinent background checks regarding the owner or owners of the building. If the building is sold during our occupancy, the same check must be made covering the new owner or owners. Be alert at all times for any information of a derogatory nature concerning the lessor which would adversely affect our continued occupancy.

2-1.2.7 GSA Leasing Procedure

(1) GSA has initiated a policy where agencies (to include the FBI) can choose GSA as their agent to procure leased space or agencies may elect to lease space under their own authority. If the choice is made to lease space under the FBI's authority, then similar procedures will be followed, with the Construction and Laboratory Contracts Unit (CLCU) providing the services that GSA would otherwise provide. The SMU shall make the final decision as to the use of GSA or the CLCU for leasing services. All previously stated procedures remain in place with this leasing avenue, with the Space Management Unit (SMU) being the program manager for any space issues. SMU will work with the CLCU to complete the space renovations and acquisition. The Facilities Management Section shall determine who the COTR shall be during requirements development and renovation stages of the project.

(2) Lease Management

(a) By Memorandum of Understanding signed by the Assistant Attorney General for Administration on October 24, 1986, and the Administrator, GSA, on January 5, 1987, the DOJ was delegated authority to perform functions with respect to the nationwide management of GSA-leased facilities under either fully serviced leases or under leases where the government has only utility responsibility. Department of Justice Order 2410.4 dated August 14, 1987, and revised by

DOJ Memorandum of May 12, 1995, redelegated that authority to the Director, FBI. This authority has been redelegated by the Director, FBI, to the Chief, Facilities Management Section; the Chief, Space Management Unit (SMU); and Space Management Specialists within the SMU at FBIHQ, and to the Administrative Officers/Office Services Managers and Supervisory Administrative Specialists within FBI field offices. Agencies having this responsibility are authorized to assign and reassign space within the building managed by them, and may contract for alterations. The delegation does not authorize agencies to lease space. It only authorizes agencies to manage space leased by the GSA. No changes to leasing authority were made by this delegation. In order to manage a GSA-leased facility, officials delegated this authority by the Director, FBI, must seek designation as Contracting Officer Representative (COR) from the GSA Contracting Officer (CO). Upon designation by the CO, the COR may assume the responsibilities of lease management.

(b) To obtain lease management responsibilities for a specific GSA-leased facility, the COR must initially contact the SMU. The SMU will provide the appropriate assistance to the COR and coordinate contact with the GSA for the assignment of GSA-leased facilities for lease management. In implementing the duties of lease management, the COR must obtain prior approval from the SMU for all assignment and reassignment of space within a lease managed facility. Additionally, all desired alterations must be approved by the SMU prior to the award of a contract for the work. The COR may initiate a request to the lessor of a lease managed facility for alterations. Afterwards, the request should be submitted to FBIHQ for final approval by the SMU. All alterations at FBIHQ will continue to be managed by the Facilities Management Section.

2-1.2.8 Rental Costs (See MAOP, Part 2, 2-1.2.10, 6-5.1, 6-8.5.1 (6)(a)6.)

The FBI is charged by GSA for space and services through rent. The services included in this charge are those normally furnished in commercial practices. GSA will furnish services additional to those included in the rent on a reimbursable basis. Charges (billings) are rendered monthly in arrears. The billing includes adjustments for billing errors and changes in space assignments made prior to or during the previous month. GSA provides these billings to FBIHQ. Copies of the printouts supporting these billings will be furnished to the field on a quarterly basis. FBIHQ will query the field to verify the accuracy of the billing data.

2-1.2.9 Deleted

2-1.2.10 Recurring Reimbursable Services (See MAOP, Part 2, 2-1.2.8, 6-5.1, 6-8.5.1 (6)(a)6.)

Recurring reimbursable services, for which separate charges will be made by GSA, will include all services performed after normal working hours, such as utilities for heating and air conditioning, and elevator services, etc. Billing for such reimbursable services will be handled by each GSA Regional Office, as opposed to the rent for space occupied which is processed at the Public Buildings Service of GSA in Washington, D.C. All matters as to certification of work authorization and funding for recurring reimbursables are to be submitted by GSA Form 2957 or FD-369 (Requisition for Services), whichever is appropriate, to FBIHQ, Attention: Facilities Management Section, for approval. Such services should be completely justified as to essential need for efficient operation. (Occasionally, standard utilities are not included in the rent, and an FD-369 must be

submitted to FBIHQ, Facilities Management Section, for these utilities as well.) FBIHQ does not sanction incurring overtime charges for resident agencies unless severe conditions exist and adequate justification is presented, such as a continuing Title III operation, after normal working hours under extremely uncomfortable conditions. Server rooms in resident agencies will be placed on 24-hour HVAC.

2-1.3 Deleted (See *Security Policy Manual* at http://rmd.fbinet.fbi/ppu/manuals-desk/manuals_published_in_new_format.htm)

2-1.3.1 Maintenance and Security of Keys

(1) Keys should be maintained in a secure manner. A designated employee should be responsible for the maintenance and security of all keys. Wherever Tel-Kee cabinets are in use, keys should be maintained in such cabinets at all times except when in actual use.

(2) A charge-out system should be maintained utilizing Tel-Kee brass receipt holders when keys are removed from the Tel-Kee cabinet or other place of maintenance for temporary periods not to exceed 30 days. If keys are charged out by any employee for an indefinite period, property receipt, Form FD-281, should be utilized. If keys are removed to be used momentarily, i.e., to open desks, cabinets, and doors at the beginning of a workday or to lock desks, cabinets, or doors at the end of a workday, charge out for this purpose will not be necessary. However, the person in charge of the maintenance of the keys is strictly responsible for their return when permitted to be withdrawn for such purpose without charge out.

(3) Keys charged out by employees are to be maintained in a secure manner.

(4) The key, keys, or combinations to all Tel-Kee cabinets or other equipment in which keys are maintained shall be available to the ranking employee on duty after regular working hours so that all keys will be readily accessible in the event of an emergency.

2-1.3.2 Deleted (See *Security Policy Manual* at http://rmd.fbinet.fbi/ppu/manuals-desk/manuals_published_in_new_format.htm)

2-1.3.3 Deleted (See *Security Policy Manual* at http://rmd.fbinet.fbi/ppu/manuals-desk/manuals_published_in_new_format.htm)

2-1.3.4 X-Ray Procedures for Screening Incoming Mail, Freight and other Related Material (See also MAOP, Part 2, 2-1.3.3, 2-2.1, and 2-2.2.)

(1) All Bureau facilities having access to or provided X- ray equipment shall use these devices to immediately screen all incoming mail, freight and related material for weapons, explosives and/or other dangerous material prior to their being opened by Bureau personnel. In conjunction with the use of the magnetometer (metal detector), X-ray machines may also be used to screen the personal possessions of non-Bureau personnel prior to their being allowed access to Bureau space, if the machine can be placed sufficiently close to the reception area. More sophisticated machines (from American Science and Engineering), capable of detecting both metallic and nonmetallic devices (and drugs) and scanning fairly large boxes, were provided to each field office not already having access to comparable equipment. Resident agencies and certain off-site facilities with listed mailing

addresses were provided smaller, conventional, parcel-size machines (from EG&G Astrophysics) that can detect metallic components.

(a) In view of the potential threat associated with the delivery of an explosive device to any of its facilities, the FBI, as a higher risk target for criminal aggression and terrorist targeting, has enhanced security of FBI offices through the use of mail X-ray screening devices.

(b) If practical, X-ray machines should be located in a controlled area that is outside protected FBI space, preferably close to the reception area and/or near the primary point of entry used by commercial carriers to deliver mail, packages, etc., to the FBI office. If there is not sufficient space and the X-ray machine must be inside the protected FBI space, delivery personnel should be requested to display proper identification and allow FBI personnel to look at the package before they depart. If absolutely required to enter interior space, delivery personnel should follow access control procedures outlined above in 2-1.3.3.

(c) The use of X-ray screening machines will enable offices to immediately screen incoming mail, freight and related material to detect weapons, explosives and/or other dangerous material. In addition, the contents of packages, bags, purses, etc., belonging to personnel entering into Bureau space, conditioned upon their consent to a weapons search of their person and possessions, may be screened by utilizing the X-ray machine.

(d) ALL packages received by FBI offices must be screened by an X-ray system prior to further distribution, to the extent an office has been provided or has access to such equipment and this equipment can accommodate the size of the package. Oversize packages are to be independently verified through use of the return address or other feasible means.

(e) The use of X-ray systems requires specialized operational training. X-ray machines shall be operated only by authorized personnel who have received proper training as offered by the manufacturer, the Bomb Data Center, or by a certified bomb technician. All mailroom personnel shall receive such training, including instructions in recognition of letter bombs and package bombs.

(f) FBIHQ and field supervisory personnel shall randomly evaluate mailroom operations to ensure that employees are properly handling and screening incoming mail, freight and related material.

(g) Suspect device procedures must be documented, prominently posted on or near the X-ray machine, and made available to all employees. These procedures shall include what course of action is to be followed when a letter or package is considered suspicious, which personnel are to be notified, and a plan for notifying the local bomb squad, when warranted. Also, appropriate security must be afforded to suspect device procedures to prevent possible compromise; that is, the posting of such information in unsecure space (i.e., loading dock, reception area, etc.) is strictly prohibited. The procedures may also include what steps to take if a suspicious package is found in the vicinity of FBI space.

(h) Personnel must be trained in and follow all associated safety instructions while operating X-ray machines. Safety and operational procedures must be scrupulously followed.

(i) If there is an indication that a package may contain an explosive device and/or other dangerous material, DO NOT MOVE OR OPEN IT The suspect package shall be left where it is and the

immediate area evacuated. Personnel who have had contact with the device shall be identified and kept available, should a bomb squad response become necessary.

(j) Posters displaying the general characteristics of package and letter bombs are available through the FBIHQ, Laboratory Division, Bomb Data Center, Extension [redacted] Room [redacted] b2

(k) If practical, given the size of the facility and the volume of incoming mail, freight and other related materials, facilities should consider using a rubber stamp or sticker to mark incoming materials with "X-rayed" in order to confirm that they have been screened for weapons, explosives and/or other dangerous materials prior to opening.

If implemented, each facility must develop its own Standard Operating Procedure (SOP). After having been reviewed by the facility Security Officer, the SOP must be approved by the division head, documented to the appropriate ACS file and made available to all division personnel. All costs associated with the implementation will be borne by the implementing facility. The following guidelines should be included in the SOP:

1. The "X-rayed" rubber stamp or sticker must be placed on the mail, freight and other related material only after it has been screened for weapons, explosives and/or other dangerous material. Placing an "X-rayed" stamp or sticker on such items prior to screening is strictly prohibited.

2. The "X-rayed" stamp or sticker must be clearly visible. It should be placed on the side of the container which bears the mailing address; however, it should not cover or obliterate any address or tracking related information.

3. The "X-rayed" rubber stamp or stickers should be afforded appropriate security. When not in use, the stamp or stickers should be stored in a manner that will avoid unauthorized use.

(2) X-RAY INSPECTION TIPS AND TECHNIQUES (For back- scatter & nonback-scatter (transmission) technology)

b2
b7E

[redacted]

b2
b7E

[redacted]

(3) TELLTALE/WARNING SIGNS

[redacted]

(4) NOTIFICATION AND REPORTING REQUIREMENTS

(a) To ensure the safety of personnel, visitors, and property, all offices shall reiterate, on a semiannual basis, the mandatory X-ray Screening Policy to all personnel as set forth in this manual citation. Additionally, each office maintaining American Science and Engineering (AS&E) X-ray equipment shall provide a reading of the volume of items inspected by electronic communication to FBIHQ, Security Division, Attention: Physical Security Unit (PSU), Room [redacted] by the close of business on 12/15 and 6/15, of each year. The actual reading shall be taken between 12/1 and 12/14, and 6/1 and 6/14, of each year. b2

(b) Upon receipt of this information, the PSU will review each reading to determine if offices are X-raying mail as required. Consideration will be given to the size of the office as well as the date of installation. The PSU is cognizant of the fact that AS&E machines have a "Special Feature" which overrides the inspection counter for an uninterrupted view of the items inspected. This feature is designed to scan a number of small items at one time when they lack density, thus, showing a count of one, when a number of items were, in fact, scanned. Offices should only use this feature on a "need-be" basis, so the PSU can accurately evaluate the use of equipment. In the event it is

determined that an office is not in compliance, the PSU will forward the information to the Inspection Division for appropriate action.

(5) TRAINING, TESTING, AND CERTIFICATION OF EMPLOYEES ENGAGED IN X-RAY SCREENING

(a) All divisions provided an Automated Multimedia X-ray Equipment Training System shall train, test, and certify all employees engaged in X-ray screening on a semiannual basis (every six months). The training system is designed to provide convenient, standardized instruction, and measurable competency on X-ray interpretation and other related subjects, thus, improving the overall security of the FBI.

The system provides the following:

1. Operation Basics - Provide a step-by-step guide to all the features of an AS&E Model 66Z X-ray Machine, with an opportunity to practice using a replica of the console.

2. Troubleshooting - Provide basic operational errors through live demonstrations and simulated troubleshooting.

3. Basic Image Training - Provide threat identification by presenting basic image analysis strategies.

4. Advanced Image Training - Provide more complicated images in a continuous X-ray scanning mode.

5. Expert Image Training - Provide additional and more complicated images, decrease the intervals between them, and allow the operators to refine their image analysis skills.

(b) Training Instructor

Each division provided an Automated Multimedia X-ray Equipment Training System shall designate a representative to be responsible to ensure all division employees who perform X-ray screening duties are trained, tested, and certified in X-ray machine operation and interpretation. The representative should have a background in training and the authority to schedule, guide, test, and certify employees.

(c) Training/Testing/Certification

1. The Training Instructor will maintain supervisor settings on the training system as set forth, upon notification, be able to modify the number and kind of images, the pass threshold, and the score weighting for each section of training.

2. The Training Instructor must be present while testing is being conducted and be able to answer questions during the Demonstration and Hands-On Sections of the training. During the Challenge Section of the five levels, no answers can be given to the operator.

TRAINING SECTION	SCORE	NUMBER OF TRIES	PASS THRESHOLD	PASS THRESHOLD

b2
b7E

[redacted] b2 b7E

3. Employees that do not pass with [redacted] will automatically be returned to the beginning Hands-On Section for that level being tested. This procedure will repeat itself until the employee passes with at least [redacted]. In determining if the employee has passed or failed for each section, the Training Instructor must not only consider the score, but also the number of tries attempted. If the employee has [redacted] or better score with two or less tries for each section, the employee has passed and is considered certified. If the employee has [redacted] or better score but has more than two tries in any section, the employee has failed. If the employee has less than [redacted] or cannot complete any section, the employee has failed. Employees that do not pass shall be removed from the duties of X-ray screening until provided additional one-on-one training. The additional training shall be provided by the FBI's Bomb Data Center or by a certified FBI Bomb Technician. Upon receipt of additional training, the employee may immediately be retested using the above passing criteria to determine if the employee is able to return to the duties of X-ray screening. Before any NEW attempt on the simulator, the old user ID must be deleted from the training system; fresh tallies are needed for each retest.

4. Each instructor must keep a record of exact user ID (first and last name) and password used by the operator. Printed test results are to be kept for three years in a secured area. Upon request, the test results must be made available to FBIHQ to evaluate the effectiveness of this training program.

5. The training system must be operated in a dedicated mode as defined in the Manual of Investigative Operations and Guidelines (MIOG), Part 2, 35-9.4.8. That is, it may be only used for the purposes as stated above. No other software or data is to be entered into, processed on, or transmitted by this computer.

2-1.4 Instructional Books or Working Guides

Each SAC is responsible for arranging the review of instructional books and working guides in such frequency as to ensure their currency and accuracy, and for maintaining an administrative tickler or other record to indicate when and by whom these checks were last made.

2-1.5 Firearms in Field Offices

Instructions regarding the maintenance of firearms in field offices and resident agencies may be found in Part II, Section 12 of the Manual of Investigative Operations and Guidelines (MIOG).

2-1.6 Smoking in Bureau Space

(1) The Department of Justice Property Management Regulations, Title 41 of the Code of Federal Regulations, Chapter 128, Subpart 128-20.1, prohibits smoking in all Department of Justice work places to ensure that personnel are not exposed, involuntarily, to environmental tobacco smoke at the work site. In part, these regulations state:

"Environmental tobacco smoke, also known as second-hand or passive smoke, has been identified by the Environmental Protection Agency as a major source of harmful indoor air pollution and a

known cause of lung cancer, respiratory illness, and heart disease. The purpose of the following is to provide Department of Justice employees with the safest work environment possible.

"This policy applies to all (FBI) personnel, visitors, contractors, and personnel of other agencies and businesses that operate within or visit (FBI) workplaces.

"Environmental tobacco smoke (is the) exhaled and/or side stream smoke emitted from smokers in the burning of cigarettes, cigars, and pipe tobacco (and is) a major source of harmful indoor air pollution and known cause of lung cancer, respiratory illness and heart disease.

"Workplace is defined as any (FBI-owned) or that portion of any (FBI-leased) building where work is performed by (FBI) personnel, (or) any vehicle acquired by the (FBI) for its personnel. (The new smoking policy is) to protect all (FBI) personnel from health hazards caused by exposure to tobacco smoke. (It bans) smoking of tobacco products in all (FBI) workplaces.

"Since environmental tobacco smoke is classified as a potential occupational carcinogen, exposure to environmental tobacco smoke must be reduced to the lowest feasible concentration; therefore, smoke break areas shall only be outdoors and twenty-five (25) feet away from common points of ingress and/or egress into the workplace. Indoor designated smoking areas are prohibited." (See MAOP, Part 1, 13-13.)

(2) Since this smoking policy is not intended to interrupt any undercover operations, each SAC and Assistant Director may use his/her discretion to control smoking in undercover vehicles and/or other workplaces.

(3) Initially, and if the circumstances permit, employees should be encouraged to resolve any problems regarding smoking in work areas among themselves or through their respective supervisors. In sensitive circumstances, such as where an employee fears retribution or retaliation should they voice their objection or lodge a complaint concerning the violation of the Bureau smoking regulations, the employee may contact the Occupational Safety and Environmental Program Unit, Administrative Services Division (ASD), FBIHQ, or a designated official in that office, to report a violation of the Bureau smoking regulations.

(4) The Occupational Safety and Environmental Program Unit, ASD, FBIHQ, or their designated official, shall be responsible for obtaining as many facts as possible from the complainant or objector, and when appropriate, forwarding the facts without disclosing the identity of the objector or complainant to the appropriate FBIHQ Section Chief, Assistant Special Agent in Charge, or other designated official for further investigation. Should the above official be the subject of the complaint or objection or other sensitive circumstances exist making referral to that official inappropriate, the Occupational Safety and Environmental Program Unit or their designated official shall refer the matter to the official's supervisor or other appropriate official.

(5) Upon receiving a referral from the Occupational Safety and Environmental Program Unit, ASD, FBIHQ, each FBIHQ division, office, or field office shall conduct the necessary investigation to either corroborate or refute the objection or complaint, and if corroborated, either correct the problem or document a violation of the Bureau smoking regulations and shall be responsible for referral of violations of Bureau policy for appropriate action to the Adjudication Unit, Office of Professional Responsibility, FBIHQ.

2-2 RECORDS MANAGEMENT

Field offices must be operated strictly in accordance with Bureau instructions relating to Records Management. The Special Agent in Charge (SAC) in each field division (Administrative SAC in New York Division) is designated the "Custodian of Records." In the absence of the SAC, related responsibilities may be designated to the Assistant Special Agent in Charge (ASAC).

2-2.1 General Instructions for Receiving Mail and Related Material (See MAOP, Part 2, 2-1.3.4.)

(1) All incoming mail, freight, and related material must be received directly from its respective mailing/shipping representative, or by the use of an official United States Postal Service (USPS) Post Office (PO) Box. Utilization of a third party (i.e., security guard, adjacent office (non-FBI), other government agency, commercial store front mailing establishment, etc.) to accept incoming mail, freight, and related material on behalf of the FBI is strictly prohibited.

(2) All Bureau facilities having access to or provided X-ray equipment shall use these devices to immediately screen upon receipt all incoming mail, freight and related material. Packages which cannot be X-rayed due to their size must be independently verified as legitimate through the use of a return address or other feasible means. Offices should not disregard a suspicious package even though it may be labeled with a Bureau mailing label. Labels can be easily duplicated and used as a possible camouflage technique by bombers to deceive the recipient.

(3) All incoming mail, freight and related material must be immediately inspected as it is received, paying particular attention to any indications of possible compromise. Packages received opened or damaged in such a way as to where the contents could have been easily removed must be immediately reported to the Division Security Officer for appropriate action. A subsequent electronic communication shall be sent to FBIHQ, Security Division, Attention: Physical Security Unit, Room 4266, and Administrative Services Division, Attention: Mail Services Unit, Room 1B006, providing pertinent details of the incident. Security questions regarding USPS procedures may be directed to the local Postal Inspector. Security questions regarding FedEx procedures may be directed to FedEx Security Dispatch, Memphis, Tennessee, by calling (901) 922-1945.

(4) X-ray systems are technical equipment and require special operational training. X-ray machines shall be operated only by authorized personnel who have received proper training as offered by the manufacturer, the Bomb Data Center, a certified bomb technician, or by the use of the automated multimedia X-ray training system (see MAOP, Part 2, 2-1.3.4 (5) for further details. All mail room personnel shall receive such training, including instructions in recognition of letter bombs and package bombs.

(5) Personnel must be trained in and follow all associated safety instructions while operating X-ray machines. Safety and operational procedures must be closely followed.

(6) FBIHQ and field supervisory personnel responsible for mail processing shall randomly evaluate mail room operations to ensure that employees are properly handling and screening incoming mail, freight and related material. Such evaluations shall be documented and made available to the Security Division upon request.

(7) Suspect device procedures must be documented, prominently posted on or near the X-ray machine, and made available to all employees responsible for examining mail, packages, etc. These procedures shall include what course of action is to be followed when a letter or package is considered suspicious, which personnel are to be notified, and a plan for notifying the local bomb squad, when warranted. Also, appropriate security must be afforded to suspect device procedures to prevent possible compromise. That is, the posting of such information in unsecure space is strictly prohibited.

(8) If, when screening packages, a particular package arouses suspicion, employees should utilize the following steps to clarify a potential threat:

(a) Contact the intended recipient to determine if the package is expected. If the recipient is not expecting a package from the stated sender, proceed to 2-2.1(8)(b). If the recipient can identify the contents of the package and this can be compared successfully as a nonthreatening item with the X-ray, then the package can be released.

(b) If the suspicious item has an FBI return address, contact the stated sending Bureau office to determine the sender and a description of the contents of the package. If the FBI sender can confirm the tracking number as an actual shipment from their office, provide a successful identification of the contents, and this can be compared successfully as a nonthreatening item with the X-ray, then the package can be released.

(c) If the sender cannot be verified or identified, the sender is an outside source, or if the FBI sender is not capable of providing information on the shipment, continue to consider it suspicious and follow procedures detailed under 2-2.1 (9).

(9) If there is an indication that a package may contain an explosive device, the following steps shall be immediately taken:

(a) DO NOT MOVE OR OPEN THE DEVICE. The suspect package shall be left where it is and the immediate area evacuated. Personnel who have had contact with the device shall be identified and kept available, should a bomb squad response become necessary.

(b) Notify the appropriate personnel in the chain of command. Each office shall have an emergency contact list with the telephone numbers of the appropriate personnel in the office to notify. This list should include the Special Agent Bomb Technician for the division who may be able to provide further diagnostic abilities and coordinate with the bomb squad response if necessary.

(c) Avoid changing the environment of the package. Do not expose it to heat, cold, moisture, or other environmental factors. No transmitters, including radios, cellular telephones, two-way pagers, or other radio frequency-producing equipment should be used in the vicinity of the device. Radio transceivers can generate an electrical field which may be sufficient to cause an improvised explosive device to function.

(d) Under no circumstances should any mail room employee attempt to open a suspect package. Such actions must be accomplished by appropriately trained personnel.

(10) Posters displaying the general characteristics of package and letter bombs are available through the Bomb Data Center, Laboratory Division, Quantico, Virginia, [redacted] Room [redacted] b2

(11) In addition to the mail security requirements as set forth in MAOP, Part 2, Section 2-2.2, all FBI offices shall institute procedures wherein incoming U.S. Mail from sources outside of the FBI (including other government agencies) are opened and inspected for any foreign substance in a Biological Safety Cabinet (BSC).

(a) A foreign substance is defined as an abnormal or improper item or material transported in the mail. Foreign substances include, but shall not be limited to, powdery or crystal substance(s), solid particle(s), liquid, fluid, gas, or an item or material having some type of odor. Any of these or similar types of substances shall be considered suspicious. In addition, containers designed to hold liquids, gases, and biological material (i.e., vials, petri dishes, etc.) shall also be considered suspicious and handled accordingly.

(b) Employees using a BSC for opening U.S. Mail shall wear protective gloves (e.g., disposable gloves, 100 percent Nitrile, 6-mil, 11 inches in length). Protective gloves that do not come in contact with contamination may be disposed of in regular trash.

(c) After initially screening incoming mail for explosive devices and other hazardous material, Bureau offices shall immediately and visually inspect the outer wrapping of all U.S. Mail with respect to the following:

1. Evidence of a foreign substance
2. Excessive postage
3. Handwritten or poorly typed address
4. Incorrect titles
5. Title, but no name
6. Misspelled common words
7. Oily stains, discoloration or odor
8. No return address
9. Possibly mailed from a foreign country
10. Lopsided or uneven envelope
11. Protruding wires or aluminum foil
12. Excessive wrapping material such as tape, string, etc.
13. Marked with restrictive endorsements, such as "Personal," "Confidential," to be opened by addressee only, etc.

(d) If, when visually inspecting mail, a particular piece of mail resembles any of the above profile, it shall be considered suspicious. Employees shall utilize the following steps prior to the opening of such mail in a BSC to minimize exposure to a possibly harmful substance.

1. Do not shake, smell, blow on, or open the letter or package.

2. Place the envelope or package in a clear sealable plastic bag or some other type of clear sealable container to prevent leakage of contents. Rubbermaid and other similar type products are suitable containers to temporarily seal suspicious mail.

3. Mail which cannot be put into a plastic bag or some other type of sealable container due to its size, shall be moved and placed into the provided BSC. The BSC shall be immediately turned on and then the mail opened and inspected for any foreign substance.

(e) While visually inspecting incoming mail, employees shall separate incoming mail into two categories, 1) suspicious, and 2) nonsuspicious. Mail defined as suspicious shall be given top priority and opened first in a BSC. After the mail defined as suspicious has been opened and inspected, all other U.S. Mail shall be opened and inspected in a BSC in the following order:

1. Accountable (USPS Express, Registered, Certified, etc.).

2. First Class and Business Reply.

3. Bulk Rate, Periodicals, Magazines, etc.

(f) Once the mail has been opened in a BSC, employees shall remove the contents from the envelope/packaging material and thoroughly inspect both the contents and envelope/packaging material for any foreign substance. If mail being inspected has additional inner envelope(s)/packaging (one inside the other), the inner envelope(s)/packaging shall also be opened and inspected for any foreign substance. If no foreign substance is found in the mail, the contents may be placed back into the original envelope/packaging material and re-sealed with tape and/or staple(s) to prevent the contents from falling out and getting lost. The resealed mail may then be removed from the BSC for forwarding to the mail room for additional processing and delivery.

(g) Mail with no outer wrapping, such as periodicals, magazines, etc., shall also be inspected for any foreign substance by "fanning" the pages. If no foreign substance is found, such mail may be removed from the BSC for forwarding to the mail room for additional processing and delivery.

(h) Offices may consider using an "Opened and Inspected" rubber stamp or sticker, to the extent it is practical considering the size of the facility and the volume of mail received, to confirm items have been examined and verified as not containing a foreign substance. If implemented, each facility must develop its own Standard Operating Procedure (SOP). The SOP shall be documented, approved by the Division Head, and made available to all employees. It is recommended that the following guidelines be included in the SOP:

1. The "Opened and Inspected" rubber stamp or sticker must be placed on the item only after it has been successfully verified as not containing a foreign substance. Placing an "Opened and Inspected" stamp or sticker on the item prior to inspecting is strictly prohibited.

2. The stamp or sticker must be clearly visible and be placed on the address mailing side of the item, not covering any addressing or tracking number information.

3. "Opened and Inspected" stamps and stickers must be afforded appropriate security, ensuring no unauthorized use.

(i) Mail received via a commercial carrier (i.e., FedEx, UPS, DHL, Airborne, etc.) shall also be immediately and visually inspected after it has been X-rayed for the suspicious profile stated in 2-2.1(11). If, when inspecting the outer wrapping of commercial carrier mail, a particular piece of mail resembles the suspicious profile, it shall also be processed and opened in a BSC. At the Division Heads discretion, commercial carrier mail that does not meet the suspicious profile may be transported to the mail room unopened for processing, sorting, and delivery. Whether the Division Head decides to or not to have all commercial carrier mail opened and inspected in a BSC, the same procedures stated in 2-2.1(11) shall be adhered to for commercial carrier mail.

(j) Mail received by the U.S. Mail or other commercial carriers which contains evidence shall also be immediately and visually inspected after it has been X-rayed for the suspicious profile stated in 2-2.1(11). If, when inspecting the outer wrapping of evidence, a particular piece of evidence resembles the suspicious profile, it shall also be processed and opened in a BSC. Evidence that does not meet the suspicious profile may be transported to the mail room unopened for processing, sorting, and delivery.

(k) If a foreign substance is found while inspecting mail in a BSC, employees shall immediately do the following:

1. Do not shake, smell, blow on, or empty the contents of any suspicious envelope or package.

2. Do not turn the BSC off.

3. Do not remove the envelope or package from the BSC.

4. Do not attempt to clean up the foreign substance.

5. Place the envelope or package immediately in a clear sealable plastic bag or some other type of clear sealable container.

6. Remove protective gloves and leave gloves in the BSC.

7. Leave the room and close the door, securing the area to prevent others from entering.

8. Wash your hands immediately with soap and water to prevent spreading of any suspect material to your face or other parts of your body.

9. Notify appropriate personnel in chain of command.

10. Identify personnel who have been in contact with the letter or package prior to screening and keep them available should an emergency response become necessary.

11. Remove any contaminated clothing as soon as possible and place in a clear sealable plastic bag or some other type of clear sealable container.

12. Shower with soap and water as soon as possible. Do not use bleach or other disinfectant on skin.

(l) If a foreign substance is found while processing mail outside of a BSC, employees shall immediately do the following:

1. Do not shake, smell, blow on, or empty the contents of any suspicious envelope or package.

2. Do not attempt to clean up the foreign substance.

3. Cover the spilled contents immediately with something (e.g., plastic, clothing, paper, trash can, etc.) and do not remove the cover.

4. Place the envelope or package immediately in a clear sealable plastic bag or some other type of clear sealable container and leave at the location of the release.

5. Remove protective gloves and leave gloves at the location of the release.

6. Leave the room and close the door, securing the area to prevent others from entering.

7. Wash your hands immediately with soap and water to prevent spreading of any suspect material to your face or other parts of your body.

8. Notify appropriate personnel in chain of command.

9. Identify personnel who have been in contact with the letter or package prior to screening and keep them available should an emergency response become necessary.

10. Remove any contaminated clothing as soon as possible and place in a clear sealable plastic bag or some other type of clear sealable container.

11. Shower with soap and water as soon as possible. Do not use bleach or other disinfectant on skin.

(m) Mail processing and foreign substance inspecting procedures shall be documented, prominently posted on or near the BSC, and made available to all employees. These procedures shall include what course of action is to be followed when processing, opening, and inspecting mail, which personnel are to be notified when a foreign substance is found, and a plan for notifying appropriate local emergency/safety authorities, when warranted. Also, appropriate security must be afforded to mail processing and inspecting procedures to prevent possible compromise. That is, the posting of such information in unsecured space is strictly prohibited.

(n) FBIHQ and field supervisory personnel shall randomly evaluate mail room operations to ensure that employees are properly handling and screening incoming mail for any foreign substance. Such evaluations shall be documented and made available to FBIHQ upon request.

(o) BSCs are technical equipment and require special operational training. BSCs shall be operated by only authorized personnel who have received proper training as offered by the manufacturer, safety officer, or hazardous material specialist. All mail room and other designated personnel shall receive such training, including instructions on the proper use of protective clothing and equipment.

(12) All Bureau offices must maintain a written log of all incoming Accountable mail (i.e., USPS Express, USPS Registered, USPS Certified, FedEx, etc.) received for possible tracing purposes. Bureau offices equipped with FedEx automation equipment may record incoming FedEx packages by using the FedEx satellite/computer system. Bureau offices must generate a written record from the FedEx automation equipment of incoming packages with the initials of the employee who records each package. Bureau offices not equipped with FedEx automation equipment must record incoming packages by using an FD-211. All incoming USPS Registered, USPS Express, and USPS Certified packages not recorded on USPS Form 3883 (Incoming Registered Mail) must be recorded by using an FD-211. All records may be destroyed on a monthly basis when they are at least two years old. (See MAOP, Part 2, 2-4.5.15.)

(13) Prior to disposal of empty packaging containers, all address mailing labels (i.e., standard penalty envelopes and labels, USPS and commercial carrier labels and airbills, etc.) must be destroyed or defaced, ensuring no further use.

(14) All empty inner envelopes/wrapping material with any Bureau marking must be disposed of in official trash receptacles.

2-2.1.1 Opening of SAC Mail

(1) Mail marked "Personal," whether addressed to the SAC by name only, title only, or both, must be opened only by the SAC.

(2) In the absence of the SAC, the acting SAC may open mail marked "Personal Attention," whether addressed to SAC by name only, title only, or both.

2-2.1.2 Mail Opened by Support Personnel

(1) Mail addressed to the SAC by title only, by name and title, or by name only provided it does not appear to be personal in nature, may be opened by support personnel.

(2) When mail indicates enclosures, the person opening the mail must determine whether they have been received.

(a) If so, the initials of the person opening the mail must be placed adjacent to the word "Enclosure" or the abbreviation "Enc." If enclosures are received at a later date, note the date received.

(b) If not, a notation is made on the communication to that effect; FBIHQ or submitting field office should be immediately advised.

2-2.1.3 Block Stamping Mail

Block stamps and serial stamps are no longer required on any document. Automated Case Support (ACS) automatically keeps a log on everything done such as when a document was uploaded, received in an office, and when an index record was added.

2-2.1.4 Teletypes and Telegrams

(1) Handling during business hours -

(a) Immediate teletypes must be time-stamped as soon as received and hand carried to the SAC or person acting for him/her. Other teletypes and telegrams must be time-stamped as soon as received, indices checked, and if file exists and is available it shall be attached and both file and communications routed to supervisory personnel at once.

(2) Handling during nonregular business hours -

(a) Immediate teletypes must be communicated to the SAC or person acting for him/her immediately.

(b) Priority teletypes - If Agent is on duty, Agent may use his/her discretion as to whether to communicate the teletype to the SAC or ASAC. If support personnel are on duty, they must communicate teletypes to supervisory personnel.

(3) Filing of teletypes -

(a) File FD-36 in the case file

(b) Deleted

(c) When a teletype containing the same text is sent individually to more than one field office, only the FD-36 is to be filed.

(d) Carbon of machine copy of transmitted message may be retained for one month and then destroyed.

2-2.2 General Instructions for Mailing/Shipping (See MAOP, Part 2, 2-1.3.4, 2-2.1.)

(1) The sending office is responsible for making appropriate mailing/shipping determination ensuring mailing/shipping methods are properly used. Use cheapest mailing/shipping method which will suffice in each instance.

(2) All FBI information (documents and related material up to and including the secret level) must be shipped by FedEx, U.S. Postal Service (USPS) Registered, or USPS Express between Bureau offices within the United States and Puerto Rico. The use of USPS Express must be limited only to locations not covered by FedEx (Post Office boxes, etc.). Under no circumstances should Top Secret or Sensitive Compartmented Information be sent via USPS, FedEx, UPS, etc., regardless of the destination point.

(3) Mail should not be insured. Insurance payments are prohibited by Title 40, USC, Section 726.

(4) Mail in smallest possible envelope which adequately protects the material at the least possible cost. Basic envelope selection guidelines are:

(a) Use a 4 1/8 X 9 1/2 inch envelope whenever possible. Envelope shall not be more than 1/4 inch thick so it can be processed on postal high-speed optical character readers and bar code sorters. This dimension might consist of five sheets of 8 1/2 X 11 bond paper, or ten sheets of 8 1/2 X 11 tissue paper, or an equivalent combination.

(b) Fold material to be mailed--unless too thick or cannot be folded without being damaged--to fit into the smallest size envelope, without overstuffing.

(c) Window envelopes shall not be used for the following:

1. Classified material

2. Material relating to National Security

3. Material highly confidential to the FBI or addressee

4. Addressee is a high-level government or private sector official

(d) Choose an envelope only slightly larger than the material to be mailed, to minimize shifting within the envelope.

(e) Consolidate multiple mailings made on the same day to the same address in one envelope, instead of using a separate envelope for each item.

(f) When bulk or size of mail requires a large envelope/wrapping (9 1/2 inches by 12 inches or larger), or mail is classified, double envelopes/wrapping must be used, one inside the other, to guard against mail breaking open in transit. The inner envelope/wrapping shall have the same address and return address as the outer address mailing label/airbill. Whenever the envelope/ package contains classified information, the inner envelope/wrapping shall also be clearly marked with the highest classification level. Under no circumstances shall the outer envelope/wrapping have any indication of the classification level of its contents.

(5) If possible, all information destined to a Legal Attache (Legat) must be transmitted by electronic communication (EC) or secure facsimile. Information which cannot be transmitted to a Legat by EC or secure facsimile must be sent to JEH, FBIHQ for forwarding purposes. No direct shipments of classified and unclassified-sensitive material to Legats are allowed. Unclassified-sensitive material is information that, if disclosed, could adversely affect the ability of the FBI to accomplish its mission. Examples of unclassified-sensitive information might be the identity of FBI personnel, names of individuals or groups under investigation, technical and automation equipment, or personal data on individuals. It is noted that all mail and related material sent to other countries by unsecure methods (i.e., FedEx, UPS, DHL, USPS Express, USPS Registered, etc.) may be inspected and opened by their respective customs officials; therefore, offices must be cognizant that unauthorized inspection by the host country of classified or unclassified-sensitive information can endanger people, hamper investigations, misdirect resources, and cause embarrassment.

Whenever sending Legat information to JEH, FBIHQ for forwarding purposes, put the information in an envelope and seal. Indicate the appropriate Legat destination point and classification level (unclassified-not sensitive, unclassified-sensitive, confidential, or secret) on the envelope. If the information being forwarded to a Legat has an "original" communication destined to FBIHQ for action/information purposes, attach the sealed envelope to the original communication and indicate next to the Legat copy designation "sealed envelope attached."

Once FBIHQ receives information for forwarding to Legats, FBIHQ will separate the information into two categories, (1) classified and unclassified-sensitive and (2) unclassified-not sensitive. The classified and unclassified-sensitive information will be shipped via the Department of State Classified Diplomatic Pouch System. The unclassified-not sensitive information will either be shipped via the USPS Express mail service or other acceptable commercial express services. This procedure will expedite unclassified-not sensitive material to Legats and ensure the safe shipment of classified and unclassified-sensitive material.

(6) Because of the Bureau's mandated responsibilities, FBI offices are constantly sending/receiving hoax explosive devices (usually evidence), explosive components, hazardous substances, and other dangerous materials which, when X-rayed, might appear suspicious. When offices screen all incoming items, they will experience tense situations as a result of these items being shipped. Offices should not disregard any suspicious package, even though it may be labeled with a Bureau mailing label. Labels can be easily duplicated and used as a possible camouflage technique by bombers to deceive the recipient. (See MIOG, Part 2, 13-16.6.)

(a) To identify these possible suspicious-looking items prior to receipt and minimize possible disruption of the workplace, a "Mail/Package Alert" Form (FD-861) must be used.

(b) Prior to mailing/shipping items between Bureau offices which, when X-rayed, might appear suspicious, an immediate teletype must be sent or a telephone call made to the recipient. The teletype or telephone call should identify the shipping method (United States Postal Service Registered, FedEx, etc.), identifying/tracking number, office of origin, description of contents, date it was mailed/shipped, and any other information which may be beneficial to the recipient.

(c) Upon receipt of the above-mentioned information, the recipient must complete an FD-861 and post it on or near the X-ray machine in a conspicuous manner. It is the responsibility of each office to designate an appropriate area for the posting of such information and advise all employees responsible for X-raying incoming mail and related material of the designated area. Also, appropriate security must be afforded to the Mail/Package Alert Forms to prevent possible compromise. That is, the posting of such information in unsecured FBI space (i.e., loading dock, reception area, etc.) is strictly prohibited.

(d) The form must remain posted at all times until the item in question is received. Upon receipt of the questionable item, the FD-861 should be removed from the X-ray machine or designated area, and the bottom portion of the form completed (initials of the employee who identified the package and date received). The completed form should be retained for 90 days. Thereafter, the form should be disposed in official receptacles.

(e) The same procedures apply for mailing/shipping to the J. Edgar Hoover (JEH) FBI Building. An immediate teletype must be sent to FBIHQ, Attention: Mail Services Unit (MSU), Room 1B006, or call [redacted] (8 a.m. - 4:30 p.m., EST) or [redacted] (24 hours a day, seven days a week). The MSU will be responsible for ensuring appropriate JEH FBI personnel are advised of the questionable item. b2

(f) When mailing/shipping possible suspicious-looking items OUTSIDE the Bureau, offices should make a courtesy telephone call to the recipient, providing the same information as described above (i.e., shipping method, identifying/tracking number, date sent, description of contents, etc.).

(g) Each office (including resident agencies and off- site facilities) should designate at least two employees to serve as points of contact for this matter. This will ensure that a possible communication breakdown will not occur and appropriate personnel are notified in a timely manner. Offices should consider telephone operators, mailroom personnel, and/or the supervisor responsible for managing mail X-raying screening equipment to serve as a point of contact. (7) When mailing/shipping individual hard drives (removed from or to be installed in a computer) double boxes must be used, one inside the other, to prevent the contents from breaking open in transit. The boxes must be structurally sound, with no holes, tears, or missing flaps. The use of "banker" or "photo copy" type boxes are strictly prohibited. These type boxes are designed for storage, not mailing/shipping purposes.

(a) A strict limit of no more than 20 hard drives shall be placed in one box. Prior to sealing both the inner and outer boxes, all unused space in each box must be filled with brown wrapping paper, newspaper, bubble wrap, or any other acceptable packaging filler to prevent the contents from shifting and breaking open in transit.

(b) Both the inner and outer boxes shall be sealed with plastic or gummed-paper tape so that all holes and seams on the outer finish (including loose (opened) flap joints and permanently glued

joints) are covered. Thereafter, at least four separate continuous strips of nylon-reinforced filament tape must be placed around both the inner and outer boxes. Each strip must completely encircle the box at least once, and at least three of the strips must encircle the container at a right angle to loose (opened) flap joints.

(c) The inner box shall have the same complete mailing/shipping address and return address information as the outer box. Whenever mailing/shipping classified hard drives, the inner box shall also be clearly marked with the highest classification level. Under no circumstances shall the outer box have any indication of the classification level of its contents.

(d) All hard drives up to and including the "Secret" level shall be shipped by FedEx, United States Postal Service (USPS) Registered, or USPS Express within the United States and Puerto Rico. USPS Express shall be limited only to locations not covered by FedEx (post office box address, etc.). All hard drives sent to and from Legal Attaches shall be sent by Department of State Classified Diplomatic Pouch, regardless of the classification level. Under no circumstances should Top Secret or Sensitive Compartmented Information (SCI) hard drives be sent via FedEx, USPS, UPS, etc., regardless of the destination point. Specific procedures for the transmittal of Top Secret and SCI may be found in the Manual of Investigative Operations and Guidelines (MIOG), Part 2, Section 26.

(e) Offices shall also immediately report to your Division Security Officer any lost, missing, packages received opened, or packages that were received damaged in such a way as to where the contents could be easily removed. A subsequent electronic communication shall be sent to the Security Division, Attention: Physical and Technical Security Unit, and the Administrative Services Division, Attention: Mail Services Unit, providing pertinent details of the incident.

(8) An FD-441 Receipt Card shall be enclosed in all Intra-Bureau shipments containing classified information up to and including the "Secret" level. The sending and receiving offices are to execute the appropriate portion of the form, and return the form upon receipt of the classified package within five workdays to the office of origin. If there is no other mail being sent to the office which prepared the FD-441, the form shall be sent by itself in a small, letter-size envelope by first-class mail. The use of USPS Registered, USPS Express, or FedEx to return individual FD-441s is strictly prohibited.

(9) All Bureau offices must maintain a written log of all outgoing accountable mail (i.e., USPS Express, USPS Registered, USPS Certified, FedEx, etc.) sent for possible tracing purposes. Bureau offices equipped with FedEx automation equipment may generate a written record of outgoing FedEx packages with the initials of the employee who records each package. Bureau offices not equipped with FedEx automation equipment must record outgoing packages by using an FD-211. All outgoing USPS Registered, USPS Express, and USPS Certified packages not recorded on a USPS manifest must be recorded by using an FD-211. All records may be destroyed on a monthly basis when they are at least two years old.

(10) All outgoing mail, freight, and related material must be delivered directly to their respective mailing/shipping representative. Utilization of a third party (i.e., security guard, adjacent office (non-FBI), other government agency, commercial store front mailing establishment, etc.) to deliver

outgoing mail, freight, and related material on behalf of the FBI is strictly prohibited. The use of collection boxes is also prohibited, regardless of the physical location of the box.

2-2.2.1 Mail Classes and Shipping Services

(1) Federal Express (FedEx) - The Bureau's use of FedEx small package overnight express service is provided under the General Services Administration (GSA), Contract No. GS-23F-170L, and is utilized by the Department of Justice and most other executive agencies subject to 41 CFR 101-40. The scope of the contract does NOT include "letters," i.e., ROUTINE first-class mail to a private citizen, as defined in United States Postal Service (USPS) Regulations, 39 CFR 310.1 (Private Express Statutes).

The scope of the contract also does NOT include the following for shipment: (a) Single packages greater than 150 pounds in weight and/or greater than 119 inches in length, and 165 inches in length and girth combined;

(b) Freight shipments;

(c) Same-Day shipments;

(d) Single packages smaller than 7 inches in length, 4 inches in width and 2 inches in depth;

(e) Shipments which contain both firearms and ammunition in the same package; and

(f) Shipments which may cause damage or delay to equipment, to personnel, or to other shipments.

(g) Deleted

(h) Deleted

(i) Deleted

(j) Deleted

(k) Deleted

(l) Deleted

(m) Deleted

(n) Deleted

(o) Deleted

(p) Deleted

(2) The contract specifically states that urgent letters must be delivered in accordance with the USPS Private Express Statutes which, for the most part, means that delivery must be made before 12 noon the following business day. To comply with Private Express Statutes and to receive GSA contract rates, Bureau offices must use FedEx "Priority Overnight" service with a 10:30 a.m., next-business- day delivery commitment. Using FedEx "Standard Overnight" service with a 3 p.m. next-business-day delivery commitment, or using "second- business-day" service with a 4:30 p.m. delivery commitment for FBI documents is prohibited and is in violation of Private Express Statutes and USPS regulations. Using FedEx "First Overnight" with an 8 a.m., next-business-day

delivery commitment is NOT provided under the GSA contract, but may be used only on occasions where the earlier delivery commitment is absolutely necessary. Under no circumstances should "First Overnight" be used whenever shipping to FBI Headquarters (FBIHQ). All FedEx packages destined to FBIHQ are picked up at 9 a.m. each business day regardless of the type of service indicated.

(3) USPS Private Express Statutes also require that all letters shipped express next-business-day must be marked "Extremely Urgent," or "Private Carriage Authorized by Postal Regulations," or with a similar statement. The majority of packaging containers provided by FedEx and most other express couriers are marked "Extremely Urgent." However, standard opaque packaging containers provided by GSA and commercial vendors are not marked as such. When shipping via FedEx, offices shall make sure that somewhere on the packaging container it is marked "Extremely Urgent" to comply with Private Express Statutes. (4) FedEx automation equipment must be operated in a dedicated mode as defined in the Automated Data Processing Telecommunications Security Policy, Manual of Investigative Operations and Guidelines (MIOG), Part 2, Section 35-9.4.8. That is, it may only be used to communicate, process, and store FedEx transactions. NO other software or data is to be entered into, processed on, or transmitted by this computer. All FedEx automation equipment must be labeled with a data description label (SF-711) to indicate that the equipment is contractor-owned. Bureau offices may obtain SF-711 labels from their divisions' supply technicians .

(5) Prior to sealing a packaging container, all unused space in the container must be filled with brown wrapping paper, newspaper, bubble wrap, or any other acceptable packaging filler to prevent the material from shifting and breaking open in transit.

(6) Packaging containers (i.e., envelopes, boxes, tubes, etc.) must have continuous, nylon-reinforced filament tape placed around the container from end to end and side to side as indicated below:

(a) FEDEX OR USPS LETTER (CARDBOARD) ENVELOPES

AT LEAST four separate continuous strips of nylon-reinforced filament tape must be placed around the envelope. Each strip must completely encircle the envelope AT LEAST once. Two of the strips must cover loose (opened) flap joints and permanently glued joints in a HORIZONTAL direction. Two of the strips must cover loose (opened) flap joints and permanently glued joints in a VERTICAL direction.

(b) FEDEX OR USPS TYVEK ENVELOPES

All holes and seams on the outer finish of these envelopes (including loose (opened) flap joints and permanently glued joints) must be sealed with plastic or gummed paper tape. AT LEAST two separate continuous strips of nylon-reinforced filament tape must be placed around the envelope, at right angles to loose (opened) flap joints. Each strip must completely encircle the envelope AT LEAST once.

(c) FEDEX OR USPS BOXES

All holes and seams on the outer finish (including loose (opened) flap joints and permanently glued joints) must be sealed with plastic or gummed paper tape. AT LEAST two separate continuous

strips of nylon-reinforced filament tape must be placed around the box, at right angles to loose (opened) flap joints. Each strip must completely encircle the box AT LEAST once.

(d) STANDARD OPAQUE PACKAGING CONTAINERS SHIPPED VIA FEDEX (Smaller Than 17 1/2 inches in length, x 11 1/2 inches in width, x 10 1/2 inches in depth)

All holes and seams on the outer finish (including loose (opened) flap joints and permanently glued joints) must be sealed with plastic or gummed paper tape. AT LEAST three separate continuous strips of nylon-reinforced filament tape must be placed around the container. Each strip must completely encircle the container AT LEAST once, and AT LEAST two of the strips must encircle the container at a right angle to loose (opened) flap joints.

(e) LARGE STANDARD OPAQUE PACKAGING CONTAINERS SHIPPED VIA FEDEX (17 1/2 inches in length, x 11 1/2 inches in width, x 10 1/2 inches in depth, or larger)

All holes and seams on the outer finish (including loose (opened) flap joints and permanently glued joints) must be sealed with plastic or gummed paper tape. AT LEAST four separate continuous strips of nylon-reinforced filament tape must be placed around the container. Each strip must completely encircle the container AT LEAST once, and AT LEAST three of the strips must encircle the container at a right angle to loose (opened) flap joints. The larger the container, the more strips of nylon-reinforced filament tape must be used.

(7) Packaging containers provided by the USPS and FedEx must NOT BE REUSED for shipment purposes. These containers are designed for one shipment only. Standard opaque packaging containers may be reused only when the container is structurally sound, with no holes, tears, or missing flaps. Obsolete address mailing labels and markings must be removed or covered prior to shipment.

(8) The use of "banker" or "photo copy" boxes are strictly prohibited. These boxes are designed for storage, not mailing/shipping purposes.

(9) The "release signature" block on FedEx airbill or automation equipment must NOT be executed under any circumstances.

(10) The scope of the contract provides for the shipment of hazardous materials ("Dangerous Goods"), as defined by the International Air Transport Association (IATA) Dangerous Goods Regulations. Bureau offices must comply with all federal, state, and local laws governing packing, wrapping, marking,and labeling whenever shipping dangerous goods. Specific information about dangerous goods may be found on the internet at http://www.fedex.com and searching for "dangerous goods," or by calling FedEx at (800) GO-FEDEX, selecting prompt 81 and asking for the dangerous goods department. All FBI employees/contractors that wrap/package and place into shipment a hazardous material (dangerous good) must receive general awareness/familiarization training and function-specific training regarding hazardous materials. The FBI has designated FedEx or the Department of Transportation, Transportation Safety Institute, Oklahoma City, for hazardous materials training. (See MAOP, Part 2, 2-2.2.13 and 6-2.3.9; MIOG, Part 2, 13-6.7.)

(11) All FBI FedEx invoices are received electronically at FBIHQ on a weekly basis and reviewed by the Mail Services Unit (MSU) for accuracy, compliance within the scope of the FedEx Domestic Overnight Express service contract, late deliveries, and unauthorized activity. To be in compliance

with standard Inspection Division audit guidelines, FBI field offices and other FBI locations shall receive a weekly FedEx summary statement via the FBI Intranet. This summary statement will be e-mailed directly to financial managers and other designated finance personnel. For locations that do not have a financial manager, the lead finance official of that site shall be designated as the point of contact. If the financial manager or designated finance official changes, it is the responsibility of the field office or FBIHQ location to inform the MSU of the change. In the event FBI FedEx account locations receive a paper invoice for shipments made, these invoices shall be reported by e-mail and then forwarded to FBIHQ, Attention: Ms. Dolores A. Gibbs, Program Analyst, MSU, Facilities Management Section (FMS), Administrative Services Division (ASD), Room 1B006.

Financial managers and designated personnel shall ensure that the FedEx summary statement is reviewed for accuracy within five workdays of receipt. The summary statement shall be compared with the FedEx records maintained at each FedEx account location within the division. If the statement is accurate and both records match (i.e., date of shipment, tracking number, from and to address, account number, etc.), the financial manager or the lead finance official shall download the summary page of the statement into paper form. The summary page must then be signed, dated and filed as a subfile under the master Third Party Draft control file. Records shall be maintained for a period of six years and six months. Thereafter, the records may be destroyed. If the financial manager or lead finance official identifies any incorrect charges or unauthorized shipments, these charges and/or shipments shall be reported by e-mail within five workdays to the MSU. The MSU shall reconcile any incorrect charges or unauthorized shipments with FedEx within five workdays of e-mail notification.

(12) FBI FedEx account locations are no longer responsible for identifying and informing FedEx of packages delivered outside the published delivery commitment (late deliveries). Although packages delivered after the delivery commitment will appear on the weekly summary statement, the MSU shall work with FedEx to determine if these are appropriate charges and seek the appropriate credit or refund for late deliveries.

(13) FBI FedEx account locations shall continue to be responsible for verifying the actual delivery of FedEx packages shipped within two workdays after shipment. Lost or missing packages shall be immediately reported to the division Security Officer. If the lost or missing package cannot be located within 15 calendar days, an electronic communication shall be sent to FBIHQ, Security Division, Attention: Security Compliance Unit, PA-555, and Administrative Services Division, Attention: Mail Services Unit, Room 1B006, providing pertinent details of the incident. See 261C-HQ-C1407494 Serial 153 for Security Division reporting guidelines.

(14) FBI FedEx account locations shall also continue to be responsible for identifying and informing FedEx of packages received in damaged condition and seeking an appropriate refund. Each FedEx package is automatically valued at $100 per package, or $1.00 per pound, whichever is greater. When shipping material via FedEx valued over $100, offices should declare the actual value (up to a maximum of $50,000) by indicating the value on the airbill or through FedEx automation equipment before presenting the package to FedEx. To receive a refund, FedEx must receive notification of the damaged package within 15 calendar days of the date of delivery. A damaged package notification must be made by calling (800) 463-3339, selecting prompt 0, and asking for "claims." FedEx will provide a control number and fax a claim form to the requested

location. The completed claim form must include all documentation related to the proof of value (i.e., copy of original invoice from vendor/supplier, itemized repair invoice or statement of nonrepair, appraisals, expense statement, or any other applicable documentation). The majority of claims are resolved within 5 to 21 days. Damaged package claims that cannot be reconciled with FedEx shall be brought to the attention of the MSU.

(15) To ensure the accuracy of the FedEx electronic invoicing process, all requests to open or close an FBI FedEx account shall be submitted by electronic communication or e-mailed to Dolores A. Gibbs, MSU, ASD. To open an account, the requester must provide the street address of the account location, point of contact, telephone number, justification for the account, and anticipated volume of FedEx packages sent on a daily basis. To close an account, the requester must provide the account number, street address, and point of contact.

(16) With the merger of FedEx and Kinko's into FedEx Kinko's, FedEx shipping account holders are capable of purchasing supplies and related materials by using their FedEx account number. The scope of the contract with FedEx does not include the purchase of supplies and related materials. Under no circumstances should offices use their FBI FedEx account number to purchase any supplies and related materials from FedEx Kinko's or from any other source. Supplies and related materials may be purchased by an approved government credit card or by any other authorized procurement method.

(17) When presenting packages to FedEx, offices must ensure that a complete "from and to" mailing address, the sender's and recipient's telephone numbers, date, type of service (priority overnight), weight, value (if applicable), special handling (Saturday delivery, dangerous goods, etc.), and account number are clearly printed or typed on the mailing label/airbill. Under no circumstances should offices present packages to FedEx without the above delivery information. All FedEx shipments must also have a FedEx SEL-17 exception sticker next to the address mailing label. Offices may obtain SEL-17 stickers by contacting FBIHQ, Ms. Deborah R. Brooks, or Mr. A.C. Tarver, Mail Supervisors, MSU, (202) 324-4303.

(18) FedEx account numbers are like credit card numbers and must be provided appropriate security. Offices are prohibited from providing FBI FedEx account numbers to outside sources unless it is for official business, the outside source is known and considered trustworthy (i.e., other government agencies, task forces, victims of crime, cooperating witnesses, etc.), and the shipment is made to an FBI office. Under no circumstances should FBI FedEx account numbers be provided to outside sources for unofficial purposes, for third party shipments (from and to non-FBI locations), or for the delivery of paid goods and/or services. It is the responsibility of all offices to be diligent in identifying and reporting possible fraud and/or unauthorized shipping activity.

(19) The use of FedEx is considered "Premium Transportation" and should not be indiscriminately or needlessly used. Bureau offices should use the cheapest mailing method which will suffice in each instance. Bureau offices shall use FedEx for the daily, consolidated shipment of FBI documents and related materials (up to the "Secret" level) between Bureau offices within the United States and Puerto Rico. Bureau offices may also use FedEx to other government agencies and outside sources for time-sensitive materials. However, to save funds, offices should refrain from sending FedEx packages separate from the daily, consolidated Bumail shipment unless it is absolutely necessary (i.e., size of material, hazardous material, evidence, court order, etc.). Offices

are strongly encouraged to take advantage of automation technologies already available to transmit information in lieu of FedEx. Additionally, the use of FedEx for shipment of office supplies, forms, routine, public source material, and/or items outside the scope of this contract is prohibited. Each office is responsible for making the appropriate shipping determination, ensuring FedEx is properly used.

2-2.2.2 Registered Mail

The weight and size limits for registered mail is 70 pounds and 108 inches in length and girth combined.

(1) Use registered mail for - (See MAOP, Part 2, 2-2.2.9.)

(a) Deleted

(b) Evidence

(c) Valuables - item having a reimbursable value, such as coin, currency, jewelry, etc. The reimbursable value (up to $25,000) must be declared to the postal service.

(d) Material classified under Executive Order 12958. "Secret" and "Confidential" material must be enclosed in opaque sealed envelopes where size permits or in opaque sealed boxes. Refer to MIOG, Part 2, 26-7.2, for transmitting material of this type to other agencies.

(e) Firearms - when within weight limitations (See MAOP, Part 2, 6-2.3.9; MIOG, Part 2, 12-5(5) & 13-6.7(29), for shipment of firearms.)

(f) Any other material which the Bureau has ordered sent by registered mail.

(g) Receipts for registered mail (FD-441) sent from a resident agency are to be forwarded to the field office headquarters. Field offices are to verify receipt of all registered mail and FD-441s by noting adjacent to the registered number on U.S. Postal Service Form 3877 (outgoing registered mail) or 3883 (incoming registered mail), the date and the initials of the employee who confirms the receipt of the mail and FD-441. Thereafter, the FD-441s are to be destroyed. Postal Service Forms 3877 and 3883 are to be destroyed on a monthly basis when two years old. (See MAOP, Part 2, 2-4.5.15.)

(h) Form FD-441b (Registered Mail Tracer Request) is to be used to trace and verify receipt of registered mail dispatched to an FBI office when the registered mail receipt cards have not been returned to the originating office. The receiving office is to execute the appropriate portion of the form and return it to the sending office. The information on the FD-441b will be recorded in the absence of the misplaced registered mail receipt card. Thereafter, the FD-441b may be destroyed.

(i) Form FD-441a (Receipt) is green in color and is to be used in connection with mailing evidence from one field office to another or from a field office to FBIHQ. The form is to serve as verification that the receiving office did, in fact, receive the evidence. The receiving office is to execute the appropriate portion of the form and return it to the sending office (Attention: Evidence Control Technician) where it is to be placed in an evidence envelope (FD-340, FD-340b and/or FD-340c) and filed in the 1A section of the case file for retention pending final disposition of the file. (See MAOP, Part 2, 2-4.4.11.)

(2) Numbering Registered Mail

(a) All registered mail must be numbered by a self- adhesive number preprinted, i.e., (R020043002), label.

(b) Labels should be used in numerical order and the complete nine digit number, including the prefix "R" must be recorded on the postal manifest.

(c) Labels are obtained from local post offices.

(3) Wrapping Registered Mail - Standard opaque packaging containers shipped via USPS Registered mail must be sealed in a manner that will allow application and retention of adhesive stamps, postage meter impressions and postal endorsements made by hand stamp, ball- point pen, or number two pencil. The use of masking, cellophane, nylon-reinforced, and/or plastic tape on the outer finish of registered mail is prohibited. Bureau offices must use extra gummed paper tape to ensure the registered packaging container does not break open in transit.

(4) Registered mail from FBIHQ -

(a) A record of mail received from FBIHQ must be maintained for two years on Form FD-211.

(b) Record must show date and time of receipt, accountable/tracking number, initials of employee signing postal service receipt when a return receipt is received, whether the return receipt card is Bureau Form 4-37 or whether it is U.S. Postal Service Form 3811.

(c) Enter on Form 4-37 the actual time of receipt of the mail by the Bureau employee from the post office box or the actual time the mail is delivered to the office by a postal service employee.

(d) Deleted

2-2.2.3 Express Mail (USPS)

Provides for next-day service if mailed no later than the designated time required by each post office. May be used for transmitting information classified "Confidential" or "Secret" between FBI offices within the United States and Puerto Rico. The use of USPS Express Mail must be limited only to locations not covered by FedEx (Post Office boxes, etc.). Contact your local post office for service information.

2-2.2.4 First-Class Mail (11 ounces or under) (See MAOP, Part 2, 6-2.3.9.)

(1) Receives expeditious handling and transportation and consists of mailable post cards, matter wholly or partially in writing or typewriting, matter closed against postal inspection, bills, and statement of account.

(2) Pieces of mail are not acceptable for mailing if they are LESS than any one of the following measurements:

3 1/2 inches high; 5 inches long; or .007 (Seven thousandths) of an inch thick

(3) Pieces of mail more than 1/4 inch thick do not have to measure at least 3 1/2 inches high or 5 inches long. EXEMPTED from all but the minimum thickness dimension are mailings of keys, identification cards and tags.

(4) A surcharge will be required for First-Class mail weighing one ounce or less if any one of the following dimensions are exceeded:

6 1/8 inches high; 11 1/2 inches long; or 1/4 inch thick

(5) First-Class mail weighing more than 11 ounces which requires expeditious handling and transportation should bear the notation "Priority" immediately above the address. A rubber stamp with 1/4-inch high or larger letters should be used. Size limit - 108 inches in length and girth combined. Weight limit - 70 pounds.

(6) Deleted

(7) Always use First-Class mail or Priority mail for outside source correspondence mailed to Alaska, Hawaii, and Puerto Rico. Airmail is to be used only for International Mail.

2-2.2.5 Periodical Mail (Formerly "Second-Class Mail")

Use for mailing periodicals, such as magazines, newspapers, etc., when postage is paid by permit, postage stamps, or postage-meter stamps. For details, consult the United States Postal Service Domestic Mail Manual or the FBI Mail Manager.

2-2.2.6 Standard Mail (A) (Formerly "Third-Class Mail")

Standard Mail (A) weighs less than 16 ounces. It comprises the subclasses of standard mail regular, standard mail enhanced carrier route, nonprofit standard mail, and nonprofit standard mail enhanced carrier route. These subclasses include printed matter, pamphlets, catalogs, newsletters, direct mail and merchandise. For details, consult the United States Postal Service Domestic Mail Manual or the FBI Mail Manager.

2-2.2.7 Standard Mail (B) (Formerly "Fourth-Class Mail")

Standard Mail (B) consists of mailable matter that is neither mailed nor required to be as First-Class Mail nor entered as periodicals (unless permitted or required by standard), and weighs 16 ounces or more (except special standard mail and library mail). Maximum weight is 70 pounds with a size limit of 130 inches in length and girth combined. For details, consult the United States Postal Service Domestic Mail Manual or the FBI Mail Manager.

2-2.2.8 Certified Mail (See Correspondence Guide-Field.)

Certified mail provides for a receipt to the sender and a record of delivery at the post office of addressee; it is handled the same as regular mail in transit and no record of it is maintained at the sending post office. Not available for parcels and packages. May be used for mailing material not requiring the security of registered mail but where a return receipt is desired. Not normally used in Bureau mailings.

2-2.2.9 Mail to United States Attorneys

Mail for a USA located in field office headquarters city may, at SAC's discretion, be mailed to USA unless USA's office and field office are in the same building. In such instances it should be delivered by messenger or clerk. If mailed, handle consistent with above instructions in MAOP, Part II, 2-2.2.2 (1) regarding registered mail.

2-2.2.10 Deleted

2-2.2.11 Deleted

2-2.2.12 Business Reply Mail (Moved from 2-2.2.2)

Mandatory use of business reply mail by federal agencies is required by the United States Postal Service (USPS). Official mail envelopes furnished to any person, concern, or organization, from or through whom official reply is desired, must be preprinted in a business reply mail format, as required by the USPS. Penalty Mail stamps or a postage meter impression may be applied to envelopes distributed for reply purposes in lieu of the preprinted business reply mail envelopes.

2-2.2.13 Hazardous Materials (Dangerous Goods)

(1) Items that are considered hazardous materials (i.e., explosives, gases, flammable liquids, oxidizing substance and organic peroxide, toxic and infectious substances, radioactive material, corrosives, and other miscellaneous dangerous goods) must be wrapped, packaged, labeled, and mailed in accordance with 49 CFR, Part 172; and the Dangerous Goods Regulations, International Air Transport Association (IATA), regardless of the shipping method (i.e., USPS, FedEx, UPS, DHL, etc.). (See MAOP, Part 2, 2-2.2.1 (10) and 6-2.3.9; MIOG, Part 2, 13-6.7.)

(2) All FBI employees/contractors that wrap/package and place into shipment a hazardous material must receive general awareness/familiarization training and function-specific training regarding hazardous materials.

(3) The FBI has designated FedEx or the Department of Transportation, Transportation Safety Institute, Oklahoma City, for hazardous materials training.

2-2.3 Utilization of FBI Systems for Personal and/or Unofficial Purposes; Standards of Conduct

(1) FBI mail systems may be only used to receive, internally distribute, or mail matter related to official FBI business. The receiving, internal distribution, or mailing of personal matter (i.e., correspondence, merchandise, chain letters, and/or solicitations) using FBI mail channels, materials and resources, including penalty envelopes and postage funds, is prohibited by various laws and regulations.

Using any federal agency mail system is using government property, and 5 CFR 2635.704 (a)(1) states:

"An employee has a duty to protect and conserve Government property and shall not use such property, or allow its use, for other than authorized purposes. Government property includes any form of real or personal property in which the Government has an ownership, leasehold, or other property interest as well as any right or other intangible interest that is purchased with Government funds, including the services of contractor personnel. The term includes office supplies, telephone and other telecommunications equipment and services, the Government mails, automated data processing capabilities, printing and reproduction facilities, Government records, and Government vehicles."

(2) Using penalty envelopes for other than official FBI business is prohibited by Title 18, USC, Section 1719, which states:

"Whoever makes use of any official envelope, label or indorsement authorized by law, to avoid the payment of postage or registry fee on his private letter, packet, package, or other matter in the mail, shall be fined under this title."

(3) Violations should be immediately reported and treated as any other violations of standards of employee conduct involving abuse of government property.

2-2.4 Mail Addressed to Former FBI Employees

(1) Mail addressed to an employee by name or title is presumed to be official FBI mail and intended for the employee in the FBI position held. Therefore, mail addressed to a former employee shall be forwarded to their last assigned office (i.e., unit, squad, etc.) where it shall be opened by a supervisor or a designated representative for proper disposition. If it cannot be determined where the former employee was assigned, the Mail Room Supervisor or designated representative shall either return the mail to the sender or open the mail in question. If opened, the Mail Room Supervisor or designated representative shall read the mail to ascertain subject matter and route to the appropriate office or individual for appropriate action. Once opened, United States Postal Service (USPS) regulations prohibit its return, unless it is enclosed in a new envelope or wrapper with a correct address and new postage. If the mail is clearly personal and not related to official FBI business, the mail shall remain unopened and returned to sender.

(2) All FBI employees planning to leave the Bureau shall inform all correspondents of their intended employment status prior to departure. This will significantly reduce a time-consuming research process in handling such mail.

(3) This policy is in accordance with the standards in the USPS Domestic Mail Manual at D042.4.1, and with the stated position of the U.S. Postal Inspection Service, which is as follows: "Once mail addressed to an individual at a governmental or nongovernmental organization is delivered to the organization, it is out of the USPS mail stream. From that point, the organization determines disposition. This includes opening and determining disposition of mail addressed to former employees."

2-2.5 Ordering Preprinted Mailing Envelopes, Labels, and Postcards

(1) Production of preprinted mailing envelopes, labels, and postcards are regulated by the United States Postal Service (USPS) as to formats, sizes, paper, and ink (See DOMESTIC MAIL MANUAL), and by the Department of Justice (DOJ) Unified Graphic Communications Program as to typography and styling of return address information.

(2) To ensure these regulations are followed, Bureau offices must submit an FD-369 to FBIHQ when ordering preprinted mailing envelopes or postcards regardless of quantity or cost. The FD-369 should include complete return address information as well as the quantity, size, and example of each envelope and/or postcard needed. Since the procurement process will take approximately 90-120 days depending on the type of item ordered, offices should plan ahead when submitting orders to ensure an adequate supply at all times.

(3) Offices may obtain preprinted mailing labels by submitting a routing slip with the same information as mentioned above to FBIHQ, Room 1B006.

2-3 INDEXING

2-3.1 Purpose

The purpose of indexing is to record individual names; nonindividual names, such as corporations; and property which are relevant to FBI investigations so that this information can be retrieved, if necessary, to support an efficient and effective case management system for current and future investigations. The Universal Index (UNI) also serves as an information resource to the Executive Branch of the U.S. government. Executive Branch Agencies request name searches against UNI as part of their investigations to determine suitability for employment, trustworthiness for access to classified information by U.S. government employees, contractors, licensees, grantees, military personnel and other individuals with an officially determined need for access or, in the case of aliens, eligibility to remain in the United States.

2-3.2 General Policy

(1) A general index in support of FBI administrative and investigative matters must be maintained in an automated and/or a manual environment at the field office and Headquarters levels. Only information which is relevant and necessary to accomplish a purpose authorized by statute, Executive Order of the President, or by the Constitution is to be recorded in FBI files.

(2) It is absolutely essential to include as much identifying information (see 2-3.4.1) as possible once the decision is made to index based on the guidelines in this manual. The efficiency and effectiveness of present and future index systems will be determined largely by the completeness of each index record. "Indices Popular" names, such as but not limited to, JAMES JACKSON and/or JOHN SMITH, without specific identifying data are of little or no value to subsequent users of the index.

(a) Cautions: Repetitive subject indexing within a case is not necessary and is prohibited. If case Agents and/or their supervisors require repetitive subject indexing, they must request and obtain the assistance of one of the automated investigative support systems. Indiscriminate reference indexing without specific purpose also is not acceptable.

(b) Incomplete common names (common names which do not include at least a partial first name and full last name), except for title information, as well as separate standalone address, telephone, and automobile license plate numbers, should not be indexed absent extraordinary circumstances. Such unidentifiable names and/or numbers create further information management overhead costs which are not economically justifiable now or in the future.

2-3.3 Indexing Criteria and Guidelines

There are two types of records (main and reference) included in both the automated and manual systems.

(1) Main index records are prepared on individual and nonindividual names that are the subject/focus of an investigation and property information in the title of most files. There are

exceptions in Office of Professional Responsibility matters (see MIOG, Part 1, Section 263-7), zero file matters and control file matters. It should be noted that it is only necessary to index each subject and alias(es) once in each case.

(2) Reference index records are prepared on individual names, nonindividual names and property information which are not in the title of a file and are, therefore, not a known subject/target of the current investigation. The majority of these names are found in the body of a document.

2-3.3.1 Mandatory Indexing (See MAOP, Part 2, 2-3.3.2(1), 2-3.5(2) & (3), 2-3.6.1, & 10-17.8.)

(1) CASE TITLE INFORMATION: Any information which is or should be in the title of any case file, including but not limited to all known aliases, requires the preparation of a main index record. Special attention should be afforded those files using abbreviated "et al." or "code name" titles to ensure a main index record is prepared for each subject and/or target of the investigation. The "CHANGED" title instructions (MAOP, Part 2, 10-16.7.4) must be followed in such cases.

(2) RECIPIENTS OF SUBPOENAS: When a person or the records of a person, business and/or individual of a business are subpoenaed in an FBI investigation (except if the subpoena is a grand jury subpoena), the person and/or the business to whom the records relate, including aliases, must be indexed in the general indices by the office issuing and/or serving the subpoena. To illustrate, if the records of the John Doe/ABC Company are subpoenaed from the telephone company, it is the John Doe/ABC Company, not the telephone company or the telephone company employee, that is to be indexed.

(3) INDIVIDUALS POLYGRAPHED: The names and aliases of individuals polygraphed by FBI polygraph examiners must be indexed in the general index by the field office conducting the polygraph examination.

(4) Deleted

(5) STOP NOTICES: The requesting and placing offices are required to index each name and/or item of property which is documented in a stop notice while the stop notice is in force. Once the stop notice is discontinued, the index records are to be removed.

(6) COOPERATIVE WITNESSES: The names of these individuals, including aliases, as defined in the Manual of Investigative Operations and Guidelines (MIOG), Part 1, Section 270-2, must be indexed.

(7) "ZERO" FILE MATTERS: All titles must be indexed at least one time, including all names of complainants except for names of individuals representing repetitive-type sources of information such as, but not limited to, security officers of private institutions or law enforcement officers. The titles of the separate communications in these files are indexed as references. (See MAOP, Part 2, 2-3.6.4(2)(f).)

2-3.3.2 Discretionary Indexing (See MAOP, Part 2, 2-3.6.1.)

(1) It is emphasized that all individuals who furnish information or names developed in an investigation need not be indexed. Only information that is considered relevant and necessary for future retrieval by the case Agents and/or their supervisors should be indexed. This is discretionary

and is therefore a very subjective decision-making process. Field investigators, their immediate supervisors and the Administrative Officer/Office Services Manager can be held accountable only for compliance with the mandatory indexing provisions (see 2-3.3.1).

(2) It also should be noted that all witnesses or persons interviewed or contacted by the FBI are NOT routinely indexed. Such indexing is discretionary but should not be done indiscriminately, i.e., there must be some basis for the position that the information indexed may be necessary for future retrieval. Witnesses and persons interviewed are well known to the Agent during the pending investigation and generally no useful purpose is served in connection with FBI responsibilities to have such information available in the index for future retrieval. The criteria as listed are sufficient for future investigative needs and are responsive to the Bureau's responsibilities under the name check program. To do otherwise would result in building a store of data too large to be efficiently manageable or essentially useful. The retention of extraneous data cannot be justified under the basic mandates of the Bureau.

(3) Examples of discretionary indexing:

(a) Suspects

(b) Close Relatives and Associates of Subjects

(c) Victims and Complainants: This refers to victim(s) not listed in the title of a case and/or complainants (except "Zero" files).

(d) Witnesses or Others Contacted

(e) Property: Property of value noted below which is not entered in NCIC and can be identified by unique serial numbers can be indexed only if future retrieval is considered necessary. Property without a unique serial number or other identifying number should not be indexed in the general indices except for property in the title of a file or unless extraordinary reasons exist for doing so. Examples of additional pertinent data for different types of property are noted below:

1. Aircraft: Indexing should include aircraft serial number, make, year and manufacturer's model name and/or number. Aircraft registration numbers and engine serial numbers enhance record quality, if available.

2. Firearms: Indexing should include caliber, make and model number, if known, in addition to the serial number.

3. Vehicles: Indexing should include the year, make, model number, engine and/or transmission serial numbers and the Vehicle Identification Number (VIN).

4. Currency and Other Securities: Indexing should include the serial number of any bonds, money orders, stock certificates, traveler's checks, etc.

5. License Plates: Indexing should include the number, year and state of registration.

(f) Computer Addresses: This refers to addresses used with computer-related crimes. Computer Addresses are unique electronic names and numbers. They contain periods (e.g., 133.31.22.52, KAGUNSUN2.C1.KAGU.SUT.AC.JP), and are identified as Network User Identification (NUI) or

Network User Address (NUA). Please refer to "Indexing Guidelines" on the proper way of entering Computer Addresses in the Universal Index (UNI) of the Automated Case Support (ACS) System.

(g) E-Mail Addresses: E-Mail addresses are entered with the keyword EMAIL. Please refer to "Indexing Guidelines" on the proper way of entering E-Mail addresses in UNI.

(h) Internet Addresses: Internet addresses are entered with the keyword INTERNET. Please refer to "Indexing Guidelines" on the proper way of entering Internet addresses in UNI.

2-3.4 Index Data

It is important that each and every name index record created contains as much related identifying or descriptive data as possible in an attempt to make that name unique. This will allow the future searcher the ability to efficiently and effectively identify the information sought at the index level and eliminate other names without having to review additional documentation. There are two types of index data which help make an individual name unique, namely identifying and descriptive data. Identifying data is considered more valuable than descriptive data since descriptive characteristics are subjective and change more over time.

2-3.4.1 Identifying Data (See MAOP, Part 2, 2-3.2 (2), 2-3.6.2 (1).)

The relative uniqueness of a name is determined by obtaining, documenting and indexing the following fields of information:

(1) Birth date

(2) Birth place

(3) Sex

(4) Race

(5) Social Security number

(6) FBI number

(7) Other numbers

(a) Military serial number

(b) Selective Service number

(c) Identification order number

(d) Wanted flyer number

(e) Alien registration number

(f) Immigration and Naturalization number

(g) Passport number

(h) Check circular number

(8) Chinese telegraphic code: This code has become known as the Standard Telegraphic Code (STC). In addition to indexing the Wade-Giles or Pinyin Romanized version of Chinese names, the STC number is indexed as a variation of the true name.

2-3.4.2 Descriptive Data

(1) Descriptive data includes: height; weight; color of eyes; color of hair; scars and marks; etc. This information is beneficial and may be included in the miscellaneous fields of the automated or manual records.

(2) Address and localities (state or foreign country where individual has lived, worked or traveled) can also be considered descriptive data. This information is used as an eliminating factor in volume searching matters, such as the National Name Check Program, especially when dealing with a name that appears in the indices many times.

2-3.5 Indexing Requirements of General Indices Versus Automated Investigative Support Systems

(1) All investigative documents are to be reviewed, marked for indexing, if appropriate, and the index information entered into the general index in accordance with general index guidelines. Copies of documents channelized to sub files established in major operations need not be indexed when the original file copy of the channelized document has been indexed and is filed in the main case file. The guidelines of the specific automated system are to be applied to determine entry of data into that system.

(2) Automated investigative support systems, such as the Criminal Law Enforcement Application (CLEA), the Integrated Intelligence Information Application (IIIA), the Telephone Application, and the many microcomputer applications, are investigative tools and are considered part of the central records system. Names recorded in any one of the automated investigative support systems MUST also be recorded in the general indices ONLY IF THEY MEET THE CRITERIA FOR THE MANDATORY INDEXING AS NOTED IN 2-3.3.1.

(3) In other words, names or property which fall within the guidelines for optional (discretionary) indexing can be entered in the automated investigative support systems without being entered in the general index. OFFICES HAVING NAMES IN THE AUTOMATED INVESTIGATIVE SUPPORT SYSTEMS MEETING THE MANDATORY CRITERIA IN 2-3.3.1 WHICH ARE NOT INCLUDED IN THE GENERAL INDEX ARE IN NONCOMPLIANCE WITH FBI INDEXING RULES AND REGULATIONS.

(4) INDEXING AND SEARCHING FOR TOP SECRET (TS) AND SENSITIVE COMPARTMENTED INFORMATION (SCI) RECORDS

(a) The use of FBINET to index TS/SCI records is prohibited. The Secure Data Information System (SDIS) is available for FBIHQ to index TS/SCI material. The Automated Case Support (ACS) System is used to serialize TS/SCI documents. See 242-HQ-A1078703, serials 447 and 728 for specific instructions.

(b) In order to have a search of the SDIS conducted, contact the Investigative Information Processing Unit, Special File Room Subunit at FBIHQ at (202) 324-3668.

(c) FBIHQ personnel should indicate under the Scope of Search section on Form 4-22, Information Management Section search slip, if they wish to have the SDIS searched.

2-3.6 Responsibilities

2-3.6.1 Special Agent (See also Correspondence Guide-Field, 1-10, 1-11 & 1-11.1)

The Special Agent assigned a case is the manager of that case in all aspects. It is the Agent's responsibility to ensure compliance with all appropriate laws, rules, regulations and guidelines, both investigative and administrative, from inception of the case through disposition of the evidence (unless support personnel are specifically designated with that evidence responsibility). The Special Agent receives assistance in the management of cases through support provided by the Administrative Officer (AO) or Office Services Manager, the Supervisory Special Agent or the designated Relief Supervisor, the Division Counsels and the various Agent program or specific topic advisors. (See MAOP, Part 2, 2-3.6.4(1).)

(1) Agents are responsible for obtaining the birth date for all individuals interviewed and to record that information in appropriate documentation. If the date of birth is not obtained, the reason for its absence must be documented in the interview report along with an approximate year of birth for that individual. (See also MAOP, Part 2, 10-13.3(9), and Correspondence Guide-Field, 2-4.4.4 (3).)

(2) Agents are responsible for circling (main) and underlining (reference) or instructing the stenographer or typist to circle (main) or underline (reference) in red pencil any information within the body of a communication which is covered by the mandatory indexing criteria, including aliases and identifying/descriptive data. (See MAOP, Part 2, 2-3.3.1 and 2-3.6.4(2)(b).)

(3) The Agent need not mark the specific information typed in the title of the communication. The Information Management Analyst/Clerk (IMA/IMC) will, as a matter of routine, prepare index records on names and property contained in the original title and any "CHANGED" or "CHANGED (INTEROFFICE)" titles. However, the identifying descriptive data within the body of the communication related to the title information must be marked by the case Agent on the communication. The communication is then forwarded to the IMA/IMC. (See MAOP, Part 2, 2-3.6.4(2)(b).)

(4) Specific care must be taken to ensure names which are not reflected in abbreviated titles, i.e., "et al." and "code name" titles, are indexed. (See MAOP, Part 2, 2-3.6.4(2)(b) & 2-4.3.)

(5) The Agent is also responsible for underlining (reference) names, including aliases and identifying/descriptive data, or instructing the stenographer or typist to underline (reference) in red pencil those names or other items with related identifying data appearing in the body of a communication which are discretionary items for indexing and deemed necessary for future retrieval. (See (10) & MAOP, Part 2, 2-3.3.2 and 2-3.6.4(2)(b).)

(6) The Agent to whom the case is assigned is responsible for any necessary marking for indexing of FD-302s or inserts without delay. Indexing of these communications is to be done by marking a copy of the FD-302 or insert, or by marking the communication in which copies of the FD-302 or insert are used as insert pages. (See MAOP, Part 2, 2-3.6.4(2)(b), 2-4.3.2(2), 10-13.3(9), 10-13.8, & 10-13.9, and Correspondence Guide-Field, 2-11.4(3).)

(7) Deleted

(8) Information to be indexed in teletypes, except those known to be disseminated at FBIHQ to other agencies, is to be flagged by typing (X) or (XX) symbols, in parentheses, preceding and following the information to be indexed. If the information is reference data in the body of the teletype, the (X) symbol, in parentheses, should be used. If the information relates to main index data not set forth in the title, the double (XX) symbol, in parentheses, should be used. Information carried in the caption is automatically indexed as described in 2-3.6.4. In those teletypes known to be disseminated at FBIHQ, material to be indexed should be set out in the administrative section of the communication and flagged in the same fashion as in other teletypes. (See MAOP, Part 2, 2-3.6.4(2)(b)(d) and Correspondence Guide-Field, 2-9.3.1(8)(n) 6.)

(9) Deleted

(10) Deleted

(11) Agents may not recommend closing of a case, absent extraordinary circumstances, until a full name, all available aliases and all available or reasonably obtainable identifying data for all individual subject records are recorded in the general index. (See MAOP, Part 2, 2-3.6.2(2) & 2-3.6.4(2)(d).)

(12) FBIHQ personnel (Agents, analysts, etc.) will utilize a green circle (main) or green underlining (reference) to mark information for indexing on communications not already automatically indexed (Titles). FBIHQ personnel will also mark the yellow file copy of outgoing signature communications and the original of Intra-Bureau communications, as needed. If FBIHQ data processing personnel discover that a main and/or reference record on a particular name in a particular case has already been prepared, it will only be necessary for the Information Resources Division to modify the record with new identifying/descriptive data.

2-3.6.2 Supervisory Special Agent's Responsibility

(1) The Agent Supervisor, or the Relief Supervisor, in addition to providing substantive investigative guidance, must ensure there is continual emphasis on compliance with the indexing guidelines. Once a decision is made to index, whether by Administrative Officer personnel or by the Agent, attempts must be made on all pending cases to obtain identifying/descriptive data defined in Section 2-3.4.1 and Section 2-3.4.2 of this manual. Lack of consistent compliance can be reflected in any critical elements that cover the obtaining and/or reporting of information and communications responsibilities. Agent Supervisors must also be vigilant and ensure that repetitive subject and/or indiscriminate reference indexing does not occur. If repetitive subject indexing is considered necessary and advantageous for a specific major case, use of the various automated investigative support systems must be utilized since such indexing in the general indices is prohibited.

(2) Supervisors may not approve the closing of cases, absent documented extraordinary circumstances, until the full name, all available aliases and all available or reasonably obtainable identifying data for all individual subject records are recorded in the general index. (See MAOP, Part 2, 2-3.6.1 (11).)

(3) Appropriate automated management tools to easily review indexing within a case at case review time have been designed.

2-3.6.3 SAC's Responsibility

(1) Deleted

(2) Deleted

2-3.6.4 Administrative Officer/Office Services Manager's Responsibility (See MAOP, Part 2, 2-3.6.1(3)(8).)

(1) The staff of the Administrative Officer (AO) or Office Services Manager (OSM) will, as a matter of routine, prepare index records on names, aliases, and data in the title, including "CHANGED" or "CHANGED (INTEROFFICE)" titles, and will review other incoming, outgoing, and intraoffice communications, using the following markings:

(a) A check over last name - name searched and index record found which identifies the specific case file (subject matter) of the communication.

(b) A circle over last name - name searched and no index record found which identifies the specific case file. (NOTE: The foregoing indexing markings are also searching symbols indicating the results of index check of incoming communications.)

(c) Red diagonal through circle over last name - index record now prepared on name.

(d) Red diagonal through red circle (main) or underline (reference) - index record has been prepared on name.

(2) Other responsibilities of the AO/OSM staff will include the following:

(a) If AO/OSM personnel are aware that underlined names are subject-type names, they may upgrade the marking to a main record and, if already indexed, a new record need not be prepared. It will be necessary only to modify an existing record with additional identifying/descriptive data or new serial numbers. The decision to upgrade is discretionary.

(b) Word Processing personnel should inquire of the Agent on each dictation, whenever possible, if there is any indexing to be marked and, if the response is positive, comply with the instructions in Section 2-3.6.1 (2) through (8). (See Correspondence Guide-Field, 1-11.1.)

(c) Deleted

(d) Information Management Analyst/Clerk personnel should comply with restrictions against filing serials and closing cases before indexing is completed as set forth in Section 2-3.6.1, (8) and (11).

(e) Indexing SAC memoranda, material in double zero (instructional and policy) files and administrative (i.e., vouchers, space matters, automotive maintenance, physical fitness program, etc.) files is discretionary.

(f) Material in zero files shall be fully indexed as noted in the mandatory indexing criteria, MAOP, Part 2, 2-3.3.1(7).

2-3.7 Disposition of Index Data

If and when a field office territory is realigned, the SACs and the Administrative Officers/Office Services Managers involved should contact the Information Resources Division for current policy on the handling of existing manual index cards or electronic index records. The destruction, accession and or archiving of index information is controlled by policy articulated in "The Records Retention Plan And Disposition Schedule."

2-3.8 Index Searching Procedures for New Mail

(1) When new mail is received without a file number, automated indices should be searched. If the results are positive, then a manual search is not necessary. However, if the automated search is negative, the manual indices should be searched.

(2) When new mail is received with a pre-Universal Case File Number (UCFN), the document should be searched in the automated indices. As in (1) above, if the results are positive, then a manual search is not necessary. If the automated search is negative, the manual indices should be searched.

(3) When new mail is received with a UCFN file number, the document should be searched by the case number.

(a) If the results of the automated case search are positive, the mail should be routed to the Information Management Analyst/Clerk (IMA/IMC). Direct routing to the IMA/IMC is done to eliminate redundant searching. (During the process of opening the case or modifying the title as in a "CHANGED" or "CHANGED (INTEROFFICE)" communication, all the names should have already been searched in both the automated and manual indices.)

(b) If the results of the automated case search are positive, but the new mail has a "CHANGED" or "CHANGED (INTEROFFICE)" title, only the new names need to be searched in the automated indices. Again as in (1) above, if the automated search is negative, the manual indices should be searched.

(c) If the results of the automated case search are negative, the document is searched according to the procedures in (1) above.

(4) When a case file is identified, a check is placed over the last name or file number and the file number written on the communication.

(5) When the results of the search are negative, a circle is placed over the last name or file number. Any file references "identical" or "not identifiable" with the searched information shall be recorded on the incoming communication or on the indices search slip (FD-160), whichever is the more practical. If the nonidentifiable references are numerous, they may be indicated by the notation "numref."

(6) When the search is negative, then a full search should be made on combinations, variations, and contractions, the extent of which is determined by the searching employee. As a minimum, the name "John Henry Martin" should be searched as given and as John H. Martin and John Martin. All

combinations searched must be shown on the communication or the attached search slip so that the extent of the index search is readily apparent.

2-3.8.1 Alternate Office Indices Search (AOIS)

AOIS was a separate index search which allowed a field office to search other field offices' automated indices. The current automated indices generates a universal search automatically which includes all field offices, Legats, and FBIHQ.

(1) through (3) Deleted

2-3.9 Search Slip (FD-160)

(1) Form FD-160, indices search slip, may be used during the searching procedures or it may be submitted by employees requesting a search of the indices. (Form FD-160a, continuation sheet, may be used if more pages are needed.)

(2) The employee who reviews the references listed on Form FD-160 (and FD-160a, if used) must indicate by symbol the results of the review. These symbols are:

Identical (I) Not identical (NI) Not identifiable (?) Unavailable reference (U)

(3) The search slip is to be stapled to the document to which it pertains and the document and search slip are to be filed as one serial. If there is no pertinent document, the search slip is to be serialized in the appropriate file.

2-3.10 Summary Memorandum-Serialized-Index Records

Summary memorandum was used to consolidate manual reference index records. All of the identical reference information was re-typed and placed in one communication. Once the communication was filed, all of the identical reference index records were destroyed. Since index records are entered into the automated indices, there is no longer a need to consolidate manual reference index records.

2-3.11 Charge-out Card

A charge-out card, FD-260, is to be placed in the manual indices to indicate an index card is out of file whenever the circumstances are such that the absence of a charge-out card might cause a failure to locate information in the files.

2-4 MANAGEMENT OF FILES (See MAOP, Part 2, 2-4.4.16(4)(c).)

(1) FBIHQ, field office and Legal Attache file fronts and backs are white with color-coded borders to facilitate sorting and routing and to enhance security. Form 4-596 has a BLACK border and is used for FBIHQ investigative and administrative files. Form 4-596a has a YELLOW border and is used for FBIHQ nonpersonnel files stored and maintained in the File Services Unit, Information Resources Division. Form FD-245 has a BROWN border and is used for field office criminal investigative and administrative files. Form FD-245a has a GREEN border and is used for field office informant (medium green), asset (dark green) and cooperating witness (light green) files. Form FD-245b has a BLUE border and is used for all Legal Attache office files. Form FD-245c has a RED border and is used for national security investigative files. Form FD-245d is SOLID WHITE

and is used for field office personnel files. Form FD-245d.1 has a PURPLE border and is used for medical records. FD-245d.2 has an ORANGE border and is used for security program records. File fronts and backs for Universal Case File Number (UCFN) cases are WHITE with the above-mentioned COLOR-CODED STRIPED borders.

(2) The following listing identifies applicant (*) and security-related (**) classifications. All other classifications are criminal-related or administrative in nature.

1* 65** 112** 133* 176** 218** 243** 270C** 2** 67* 113** 134** 183C** 219** 246** 270G** 3** 73* 116* 138* 185** 220** 247** 271** 14** 77* 117** 140* 191** 221** 248** 278** 35* 97** 118* 151* 199** 222** 256** 279** 37* 98** 121* 155** 200** 223** 259* 283** 38* 100** 123* 157** 201** 224** 260* 284** 39** 102** 124* 158** 202** 225** 261* 285** 40** 105** 126* 161* 203** 226** 262** 290** 61** 108** 127* 163C** 212** 227** 263** 291** 62* 109** 128* 163I** 215** 228** 265** 292** 63* 110** 130* 170** 216** 229** 266** 293** 64** 111** 132* 174** 217** 241* 268** 294** 300**

2-4.1 Investigative Files

(1) On ECs, when leads are set and the communication is uploaded, no paper is sent to the lead offices. When leads are set and the communication is not uploaded or attached enclosure(s) are not uploaded, the communication must be sent to lead offices. When no leads are set and the communication is uploaded, a copy of the communication must be sent to receiving offices. On ECs when no leads are set, additional copies should be forwarded to each individual on the Attention line. The original communications need to be sent to the OO. FD-302s, inserts, and Laboratory reports require three copies to be forwarded to the OO. When necessary indices searches have been completed, the incoming communication is then routed to the responsible supervisor for appropriate action. In the OO, matching the incoming correspondence with the investigative file before routing to the supervisor is discretionary. After any necessary administrative notations have been placed on the original document by the supervisor, the document is then routed to the Information Management Analyst/Clerk (IMA/IMC) to be acted upon as indicated by the supervisor, and filed.

(2) A copy or copies can be printed out of ECF or xeroxed to disseminate leads/information to Special Agents and support employees. These copies are not to be serialized nor charged out, and are destroyed by recipients when no longer needed. However, copies marked for indexing are returned to the IMA/IMC. Upon accomplishing the requested indexing, the IMA/IMC should destroy the copy or return it to the Special Agent, if requested. It is not necessary to transfer index markings to the file copy. These procedures are also applicable to administrative and zero files, but are not applicable to classified documents requiring special control.

2-4.1.1 Serializing

(1) Each document that is placed in an investigative file must be numbered in sequence. This number is known as the serial number and the document known as the serial. An enclosure to the document is to be given a separate serial number. Inserts or FD-302s sent or received as enclosures to another document should be given separate serial numbers. (See (2) and (3) below.)

(2) Cover page(s), report, and letterhead memorandum of evaluation should be serialized as one serial. None is an enclosure of any other.

(3) A letterhead memorandum and its accompanying letterhead memorandum evaluating sources should be serialized as one serial.

(4) When a duplicate/copy of a document is required to be filed, it is given the same serial number as the original document.

(5) Deleted

(6) When a serial is transferred from one file to another, draw a line through the classification, file, and serial numbers. Write above or below the old numbers the classification, file, and serial numbers of the file to which transferred. Place executed charge-out slip, FD-5, in the file from which serial transferred.

(7) Do not reserialize files because of transfer of serials.

(8) Copies of affidavits for search warrants and copies of complaints for arrest warrants and any affidavits thereto should be filed as serials in the case file and not in evidence envelopes.

2-4.1.2 Zero Files (0) - Nonspecific Information (See NFIP Manual, 19-03, L.)

(1) Serializing -

(a) Serialize the documents placed in them.

(b) When additional communications referring to the same subject are received, they are linked to the first communication by using the reference field in the Electronic Case File, ACS. Communications related to an already existing communication should note the existing communication in the reference field when the communications are serialized.

(2) Must be maintained for - A zero file must be opened for each classification, and contained therein is the material which does not require investigation. Since the material does not require investigation, Action Required leads cannot be set out of these files. Discretionary Action and Information Only leads can be set out of these files.

2-4.1.3 Double Zero (00) Files - Instructions and Policy

(1) Serializing -

(a) Serialize the documents placed in them. Only one copy needed.

(b) Administrative review letters and replies thereto, if any, should be filed in the double zero file for the classification involved with copies to appropriate case files when necessary.

(2) Must be maintained for - In these files, one of which is to be opened for each classification, are to be placed statutes, decisions, instructions in electronic communication or SAC memorandum form, and other documents containing instructions or policy applicable to the classification involved. Since the material does not require investigation, Action Required leads cannot be set out of these files. Discretionary Action and Information Only leads can be set out of these files.

2-4.1.4 Dead Files - No Pending Investigation

Dead files were eliminated upon the implementation of the Automated Case Support (ACS) system.

2-4.1.5 Control Files (See MAOP, Part 2, 3-4.11; NFIP Manual, 19-03, L.)

(1) Control files are separate files established for the purpose of administering specific phases of an investigative matter or program. The institution of a control file in an investigative matter or program is left to the discretion of the individual with the administrative responsibility for the particular investigative matter or program or by SAC authorization. A control file is an administrative tool for managing a particular investigative matter or program. For this reason, control files are not created in each and every investigative matter or program. Control files are not to be counted on the Monthly Administrative Report.

(2) Leads on occasion may be assigned out of control files. In circumstances where neither an investigation nor an inquiry is warranted, the FBI may ascertain the general scope and nature of criminal activity in a particular location or sector of the economy. Activity in these control files must be reviewed periodically.

(3) In order to facilitate a periodic review, a "CASE TYPE REPORT" has been made available to all offices. It lists all control files and lead activity for each file for the most recent quarter. This report has been created for use by field office management. It provides a monitoring capability to ensure that lead activity within control files is acceptable and within the Attorney General and other FBI investigative guidelines. Control files are captured in the Automated Case Support (ACS) system by entering a "C" in the "CASE TYPE" field when opening or reopening a case. This report may be accessed through the "CASE REPORTS MENU" out of the "REPORTS MENU" of the Investigative Case Management application, ACS. The Administrative Officer/Office Services Manager is required to produce this report on a quarterly basis and provide this report to the SAC for SAC's management review. In order to avoid impacting the response time during normal working hours, the request for this report should be scheduled after 6 p.m. and before 6 a.m. near the 15th of the month following the end of each quarter.

(4) When referring to the file number of a control file in communications, the file number must include the letter "C" as part of the case number to indicate the file is a control file. The letter "C" is considered part of the file number and must be used on all communications concerning control files. (Example: 105A-CE- C0012345)

2-4.2 Administrative Files

2-4.2.1 Noninvestigative Files

(1) Need not be serialized unless to do so would be enhancing to operation. (Except accident and contact files). (See MIOG, Part 1, Section 66.)

(2) Each field office is to establish a separate administrative file for the following subject matters. Administrative file covers are to be marked "ADM" in the lower right corner. Only one copy of documents designated for these files must be filed unless unusual circumstances warrant filing more than one copy. The files are to be filed in numerical sequence in the pending files section. When an administrative file is closed, it is to be filed in numerical sequence in the closed file

section. The heading and subheading of the Administrative files and the correspondence designated for these files are to be adequately indexed to assure retrievability.

CLASSIFICATION 1 - TRAINING MATTERS

MAIN HEADING SUBHEADING

Training Agents - New Training Agents - Annual Training Agents - Technical Training Clerical Training Firearms Training In-Service (or other FBIHQ training) Training Law Enforcement Conferences Training Police (General) Training Police Schools -- (individual files according to locale) (not to be carried as pending files or to be reported on monthly administrative reports)

CLASSIFICATION 66 - ADMINISTRATIVE MATTERS (See MAOP, Part 2, 2- 4.5.12, 2-4.5.13, 2-4.5.15, 2-4.5.23.)

MAIN HEADING SUBHEADING

Accomplishments Statistical Accomplishments Statistics in Process Addressograph Administrative Indexing Administrative Filing System Administrative General Administrative Office (Confined to matters relating to an individual field office) Administrative Report Monthly Ammunition Arraignment Arrests Automobiles General (If correspondence is sufficiently large, it is permissible to maintain separate files bearing following titles: Automobiles - Storage Automobiles - Gasoline and Oil, etc. Automobile accidents shall be reported in separate files bearing classification #66.) Automobiles Radio Automobiles (By individual car number - If an automobile is transferred to another field office, the file pertaining to it should also be forwarded.) Bills of Lading Incoming Bills of Lading Outgoing Charity Campaigns Check Circulars Circular Letters (See MIOG, Part 2, 21-25.4.1.) Coordinators, Use of Credit Bureau Duplicating and Reproduction Equipment Employee Compensation Office of Personnel Management Regulations Agent Injuries Films Firearms (Reports concerning the training of Agents in the use of firearms shall be filed under classification #1 - Training - Firearms.) Forms GTRs Household Goods Transportation Identification Orders Outstanding Identification Orders Correspondence Imprest Fund/Draft System Inspections Internal Revenue Service Data Interviews Inventory Jails Approved or Condemned Leave Mailing List Office Memoranda Personnel Conduct Photographic Equipment Physical Examinations Position Classification Property Nonexpendable Charge-out

System Radio CW Network Radio FM Registers (maintained for field office FD-420 and FD-420a) Report Writing Resident Agencies General Resident Agencies (individual files by location) Retirement SAC Letters and SAC Memorandums (be filed in "OO" file cabinet) Salary Matters Searches and Seizures Space Supplies Surveillances Technical Equipment Technical and Microphone Logs; Request for Surveillances (To be authorization, kept under lock and Justification Letters, and supervised by the SAC) Administrative Matters Telephones and Teletypes Transmittal Letters Checks and Bonds Visiting Employees Vouchers General Vouchers By Name of Companies Wanted Flyers Weekend and Night Duty

(3) SAC letters, SAC memorandums, and Bureau bulletins contained in administrative files should be carefully examined before they are destroyed to ensure that instructions which are still applicable and which will be of future value are retained. (See MAOP, Part 2, 2-4.5.12(33) & 2-4.5.17(4).)

(4) CLASSIFICATION - 67 -

(a) Employees' personnel files, including the Employee Medical File System (EMFS) subfile and the Employee Security subfile, are to be kept under lock and key under the supervision of the SAC. These files are to be sent to FBIHQ when an employee is designated SAC or transfers to FBIHQ. Files of employees who resign or retire shall be retained 90 days and then sent to FBIHQ where duplicate records will be destroyed immediately and nonduplicative records will be integrated into the Official Personnel Folder. When permanent or temporary indefinite employees leave to enter the military service, retain files in field office. Upon notification from the Bureau that restoration rights of an employee have expired, the personnel files are to be forwarded to FBIHQ. (See MAOP, Part 1, 24-11; Legal Attache Manual, Part 1, 4-3).

(b) The office personnel file is to be kept under lock and supervised by the SAC. This file should be indexed and serialized. Items that are to be filed in the office personnel file:

1. Data favorable or unfavorable to the office or its personnel, copies to files on individuals.

2. Recommendations for supervisory positions. Copy to be placed in individual's personnel file.

3. Recommendations for attendance at special schools. Copy to be placed in individual's personnel file.

4. Recommendations for advancement. Copy to be placed in individual's personnel file.

5. Recommendations for incentive award or commendations. NO COPY IS TO BE PLACED IN INDIVIDUAL'S PERSONNEL FILE.

6. Information concerning public officials or business contacts where no investigation is contemplated and such information should not be generally available to employees.

(5) CLASSIFICATION 80 - PUBLIC AFFAIRS MATTERS

MAIN HEADING SUBHEADING

Public Affairs FBI National Academy Public Affairs Identification Matters Public Affairs Laboratory Matters Other Than Bureau Public Affairs Public Relations Matters Public Affairs Research Matters - Laboratory (FBIHQ) Public Affairs Uniform Crime Reporting Speech Material FBI National Academy Items Speech Material Interesting Identifications Speech Material Laboratory Matters Speech Material Speech Material (File copy in case file if one maintained.)

CLASSIFICATION 94 - RESEARCH MATTERS AND GENERAL CORRESPONDENCE

See MIOG, Part 1, Section 94.

2-4.3 Filing Procedures

Original documents may be placed in file without being marked for indexing; however, indexing may be indicated on an unserialized copy of the communication and forwarded to the Information Management Analyst/Clerk (IMA/IMC). Upon accomplishing the requested indexing, the IMA/IMC should destroy the copy or return it to the Agent, if requested. It is not necessary to transfer indexing markings to the file copy.

(1) All written matter (documentary) is to be filed except routing slips. However, routing slip 1-374 shall be filed and routing slip 0-7 shall be stapled to the material to which it pertains and filed whenever it contains any instructions which should be made a permanent part of the file.

(2) Deleted

(3) Files must be bound with fasteners and covers.

(4) Write the classification and file number on the top cover in the space provided.

(5) Deleted

(6) Deleted

(7) Pending cases will be filed by classification. Within the classification, the cases may be filed either according to Office of Origin (OO) and then sequentially within the OO, or numerically without regard to the OO at the discretion of the field office. Closed files will be filed sequentially within the OO identifier. Closed files will require expansion space at 57 points, one for each field office and FBIHQ. A field office may desire to place their office designator either at the beginning or the end of closed files.

(8) Pending files are to be maintained in a unit separate from the closed files. Pending files are maintained in numbered file folders.

(9) Earlier sections of multisectioned files may be kept in the closed section.

(10) Files may not be taken from the field office without the authority of the SAC who may grant such authority only in instances of imperative necessity.

(11) Files may be withdrawn from the filing cabinets only by those employees authorized to do so by the SAC.

(12) File folders which are in good condition are to be reused whenever possible.

2-4.3.1 Maintenance of Original or Duplicate Files in Resident Agency (RA)/Off-Site (OS) Location

All files are to be maintained in the headquarters city unless the RA/OS location is in compliance with the requirements for storage of classified material. (See MIOG, Part 2, 26-5.2.) In order to maintain pending original/duplicate files in an RA/OS location, the office must have received approval for open storage of classified material by the Security Programs Manager (SPM), Security Division, FBIHQ. (For considerations addressed herein, an "off-site location" is defined as any non-RA space not contiguous with headquarters city office space and not staffed by FBI personnel 24 hours a day.) The Records Management Division (RMD), Policy and Procedures Unit (PPU), FBIHQ, must be notified by EC when files are moved to the RA/OS location.

(1) Security and Administrative Requirements:

(a) Limited to locations staffed by a Supervisory Special Agent (SSA) or Supervisory Senior Resident Agent (SSRA), with support positions allocated to the site sufficient to maintain the files. The site must have FBINET capability. No increase in support Funded Staffing Level (FSL) in an office or an RA/OS location will be granted for the purpose of administering this program.

(b) The RA/OS location must be capable of being fully secured when not manned and must be protected with an approved intrusion detection system (IDS), i.e., a system which is in compliance with a document entitled "Intrusion Detection System Standards," disseminated to all offices by Bureau airtel dated February 28, 1990, captioned "Physical Security." The system must sound an alarm at the headquarters city, but may, if desirable, also sound an alarm at the local police department (PD). Headquarters city personnel must be responsible for ensuring RA/OS Special Agent (SA) personnel and, if not a covert site or otherwise inappropriate, local police are notified of the alarm. SA personnel are to immediately respond to the alarm location and conduct an inspection of the premises to determine security status or unauthorized entry.

(c) Armed response by FBI personnel, local PD, or other appropriate armed security personnel must be as soon as possible, but must not exceed 10 minutes from the time of the alarm. This period is dictated by the time GSA-approved Class 5 security containers have been rated against physical attack.

(d) Deleted

(e) Deleted

b2

(f)

(g) Deleted

(h) The SSA/SSRA assigned to the location will ensure alarms are tested on at least a monthly basis, and such testing is to be documented in an appropriate administrative file.

(i) Deleted

(j) Deleted

(k) Top Secret or Sensitive Compartmented Information (SCI) material must not be maintained in the RA/OS unless a demonstrable operational need is shown, prior approval has been granted by the Security Programs Manager (SPM), FBIHQ, and the storage facility is in compliance with the requirements for the storage of such material (see MIOG, Part 2, 26-5, 26-5.1 and 26-5.2.1).

(l) Informant and asset files shall be maintained in the headquarters city, as shall any information which identifies an informant or asset.

(m) FCI, sensitive organized crime, public corruption, and undercover operation files are to be maintained in the headquarters city, unless the SAC or Acting SAC has personally determined on a case-by-case basis that retention of the file in the RA/OS will be necessary to the effective conduct of the investigation, and that the files can be retained in a secure manner. SACs or Acting SACs cannot delegate this authority to authorize the retention of these files in the RA/OS. Justification and authorization to retain the aforementioned files in the RA/OS are to be documented by memorandum to the case file(s) involved and personally approved by the SAC or Acting SAC.

(n) All files are to be returned to the headquarters city office within 30 calendar days of when closed.

(o) The transport of files in bulk between the office and the RA/OS, and vice versa, must be by armed SA personnel or registered mail. If by registered mail, the division head is to make a determination regarding the need for an armed escort between the post office and the RA/OS location and/or the headquarters city office. This determination must be based upon the results of a threat assessment conducted by the affected division, taking into account, among other considerations, the volume and contents of the material being transported. This assessment should be documented in an appropriate control file and personally approved by the division head.

(p) All non-Bureau personnel allowed entry into RA/OS space are to be escorted at all times, unless they have been granted appropriate clearance/access to Bureau space in accordance with established procedures set forth in MIOG, Part 1, Sections 259 and 260. Official material, both classified and unclassified, must be secured, covered, and/or otherwise protected from inadvertent disclosure to any personnel not known to possess proper authorization for access to the material.

(2) All original files, including those opened in the RA/OS, must indicate on the case record in the Automated Case Support (ACS) system that the file is located at the RA/OS. This can be done by using the Squad field or the REMARKS field. All original files retained in the RA/OS must be maintained in accordance with all provisions set forth herein regarding the management of files and communications.

(3) Procedures for Maintenance of Duplicate Files in RA/OS locations:

(a) The original communications must be retained in the original headquarters city file and are not to be charged out to or filed as a serial in duplicate file in the RA/OS. In extraordinary circumstances, serials in the original headquarters city file may be charged out and recharged on a case-by-case basis to personnel assigned to the RA/OS when it has been determined by the SSRA/SSA that the serials are necessary and enhancing to the conduct of day-to-day business.

(b) Duplicate copies of communications are to be forwarded to approved RA/OS locations for retention in the duplicate file. A stamped notation, "Duplicate Copy Forwarded to _____ (RA/OS) on (date)," is to be placed on the original of the communication contained in the headquarters city file.

(c) All communications in the headquarters city file must be serialized in headquarters city. The copy of such communications forwarded to approved RA/OS locations for maintenance in the duplicate file must also contain the corresponding serial number with the stamped notation "Duplicate Serial - Original Filed in Headquarters City File." It is not necessary to charge out the duplicate serial from the headquarters city file.

(d) In locations supported by FBINET and supervised by an SSA/SSRA, indexing should be performed contemporaneously with the opening of a case, and subsequently, as needed. Unserialized mail originated in the RA/OS may be serialized and indexed in these locations once the automated serialization has been extended to the RA/OS and adequate training has been completed. All such original communications must then be promptly forwarded to headquarters city after indexing and serializing.

(e) Serials removed from the duplicate file in the RA/OS must be charged out pursuant to existing regulations.

(f) A stamped notation, "Duplicate File Maintained In The _____ (RA/OS)," is to be stamped on the file cover of all headquarters city files having duplicate counterparts maintained in the RA/OS location.

(g) A stamped notation, "Duplicate File - Original Maintained In Headquarters City," is to be stamped on the file cover of all duplicate files maintained in approved RA/OS locations.

(h) When the investigative matter to which the duplicate file pertains is closed, the duplicate file is to be forwarded to headquarters city within 30 calendar days where a serial- by-serial match is to be made with the original file. Any serials in the duplicate file that bear "action" notations, i.e., notations issuing instructions, notations requesting action be taken, notations of certification that action was taken, etc., not appearing on the original file copy of the serial are to be matched with and filed adjacent to the original serial. Remaining serials in the duplicate file not bearing "action" notations or which have not been stamped as having historical/research value may be destroyed. The employee destroying duplicate copies of serials is to initial and date the top (last) serial in the original file and note thereon that extra copies have been purged and destroyed. (See MAOP, Part 2, 2-4.3.5 (6)(b), 2-4.5.3.)

(i) Deleted

2-4.3.2 Administrative Handling of FD-302s and Inserts (See MAOP, Part 2, 10-13.8.)

(1) Original FD-302s and inserts are to contain no markings other than the initials of the author(s) and the serial number. The original document is to be filed along with a second copy. The third copy of the document is the "Agent Copy" and is not to be serialized nor charged out, and should be destroyed by recipients when no longer needed. However, if the "Agent Copy" is marked for indexing, it is to be returned to the Information Management Analyst/Clerk (IMA/IMC). Upon accomplishing the requested indexing, the IMA/IMC should destroy the copy or return it to the Special Agent, if requested. It is not necessary to transfer indexing markings to the file copy. If additional copies are required, they may be photocopied.

(a) In nonsensitive-type cases where a Resident Agent is the case Agent, the original and copy, after being initialed, will be retained in the headquarters office, as indicated in (1) above. In the event a copy of the FD-302 or insert is necessary for work purposes in the resident agency, such must be charged out to the particular Agent.

(b) If assigned to headquarters office and the dictator is the Agent to whom the case is assigned, he/she should initial the original FD-302 and return it to the Administrative Officer/Office Services Manager with a copy to be filed as indicated in (1) above.

(c) In resident agencies, if the dictator is the Agent to whom the case is assigned, he/she should initial the original FD-302 and submit it and one copy to the Administrative Officer/Office Services Manager for filing.

(2) Indexing of FD-302s (See MAOP, Part 2, 2-3.6.1 (6), 10-13.9.)

(a) If indexing of FD-302s is necessary, and a report is not being immediately prepared, the Agent to whom the case is assigned shall use the third copy ("Agent Copy") as an indexing copy, as outlined in (1) above. If a report is being prepared immediately, indexing on the third copy of the FD-302 is not necessary; the Agent is to indicate the necessary indexing on the copy of the report.

(b) Original FD-302s and 1A envelopes are to be forwarded to the OO at time prepared and/or acquired with exception of those 1A envelopes which are to be returned to the contributor in the jurisdiction wherein they were obtained. Lead office may retain excepted 1A envelopes until they have served their purpose or until lead office file has satisfied the destruction criteria at which time these 1A envelopes should have served their purpose and should be returned to contributor. (See MAOP, Part 2, 10-13.10.)

(3) The original of an FD-302 is to be filed along with a second copy. The initialing of the FD-302 by the reporting employee constitutes the necessary authority to serialize and file. The original is to contain no markings other than the initials of the author(s) and the serial number. If prosecution proceeds by trial, the pertinent originals shall be furnished to the USA in the same manner as signed statements are furnished to the USA. A notation should be placed on the second copy showing that the original was removed for court purposes. When the FD-302 is utilized as a memorandum, it should be filed as a serial after it has been initialed for the file.

(4) When FD-302s or inserts are received by the OO from another office, the original and one copy of the FD-302 or insert are to be filed. When sending FD-302s or inserts to the OO, a transmittal communication is not needed, because the FD-302 or insert should already be serialized in the OO's file.

2-4.3.3 Charge-Out Procedures

The basis of the charge-out system is the charge-out slip, FD-5. The perforated portion of FD-5 is used to route the file or serial to employee requesting same. FD-5 must be executed when files are withdrawn for purposes other than running ticklers, use of the Administrative Officer (AO)/Office Services Manager (AO/OSM), or examination of mail by SAC, ASAC, or supervisor. When the last copy of a serial is charged out, and the serial is automated, a description of the serial is optional. If the serial is not automated, the charge-out slip must contain a description of the serial. When an employee assigned to the AO's/OSM's Office removes a serial from a file, other than a consolidated file, and prepares the charge-out slip, the classification and case numbers of the file need not be shown on Form FD-5.

2-4.3.4 Charge Out of Files

(1) Pending - FD-5 must be executed and placed in the file folders.

(2) Closed - FD-5 must be executed and clipped to a red 10 x 10 card which must be placed in the space from which the file was withdrawn.

(3) To whom may file be charged out? - To employees having a need for them. Permission of the SAC must be obtained for an Agent to charge out a file on a matter on which Agent is not assigned to work. Files are to be charged out in the name of the person who is to use them.

(4) How long may files be charged out? - Files may be charged out seven calendar days counting Saturdays, Sundays, and holidays. If transferred to another employee, recharge them. Files may be recharged once if necessary.

2-4.3.5 Charge Out of Serials

Serials may be charged out to any employee having official need for them. Serials may be charged out 60 calendar days. Serials may be recharged at end of 60 days and every 60 days thereafter if necessary. The person to whom charged must submit recharge if retained. If transferred, recharge them.

(1) Pending files -

(a) FD-5 must be executed and placed on top of the most recent serial in the section of the file from which withdrawn.

(b) Procedure on return of initialed serials to pending cases: File the serials, but if the file is not in the drawer/cabinet/rotor, put the serials in the file folder and file them on the return of the file. Destroy the charge-out slip when the serial is returned.

(2) Closed files -

(a) FD-5 must be executed and placed on top of the most recent serial in the section/volume of the file from which withdrawn and a red 10 x 10 card inserted in the file in the space from which the serial was withdrawn. If more than one serial is withdrawn from a section/volume of a closed file only one red card is to be used per section/volume.

(b) Procedure on return of initialed serials to closed cases: File the serials, but if the file is not in the drawer put the serial and red card in a blank folder which must be placed in the space from which the file is withdrawn. Upon the return of the files, file them, destroy the charge-out slip, and return the red card to supply. When a case is closed and serials are charged out, send routing slip to employee to whom charged to return.

(3) Deleted

(4) Recharge serials -

When a nonautomated serial is to be recharged and the charge-out slip contains considerable description as to the serial, the Administrative Officer/Office Services Manager may date the original charge-out slip, initial it to show that the serial has been recharged, and destroy the recharge slip prepared by the Agent.

(5) Serials permanently charged -

(a) Serials permanently charged from pending and closed files must be replaced by FD-5, fully executed and filed in place of the serial.

(b) Top Secret and/or Sensitive Compartmented Information mail which is to be permanently charged out from pending and closed files must be replaced by an FD-654, fully executed and filed in place of the serial.

(6) Files and/or serials temporarily charged -

(a) In the event it becomes necessary to forward files and related record material (indices cards) from the field office to FBIHQ for processing in connection with litigation and/or FOIPA matter, etc., such material should be duplicated for retention in the respective field office prior to forwarding the original records. This applies to all documents (including FD-192s and 1-A envelopes) in the file whether a lead office or office of origin file. Upon return of the original record(s), the duplicate material is to be destroyed unless the need to again respond to a like requirement is foreseen. In the event the exigent circumstances and/or cost of duplicating voluminous material would render the aforementioned procedure impractical, you should contact the FBIHQ Division making the request.

(b) In the event it becomes necessary to add any administrative notation to a duplicate copy of a document retained in the field office, you must first contact the FBIHQ entity to which the material is charged to ensure the original is similarly marked. (See MAOP, Part 2, 2-4.3.1 (3)(h).)

(c) Whenever any files and/or serials or other record material are to be removed from the premises of FBI space, whether or not copies are retained, Form FD-702 is to be utilized to identify the charge out.

2-4.3.6 Consolidation of Files

(1) Files are consolidated on the authority of the SAC when there are two or more files on the same subject, pertaining to related or similar matter, and handling will be facilitated through consolidation. Write "Consolidated into _____" (show new file number) on the file front of the eliminated file, and retain it in the closed files section.

When the OO changes (redesignation of OO), a consolidation is done. The new OO opens a new case and notifies the old OO of the new number. The old OO closes their case and consolidates it into the new file number. The original serials of the old OO are sent to the new OO.

(2) Deleted

(3) Deleted

(4) Deleted

(5) Deleted

(6) Deleted

2-4.3.7 Reclassification of Files

(1) When it becomes necessary to reclassify a UCFN, the old classification is crossed off the file front, and the new classification is written on the file front.

(2) Deleted

(3) Deleted

(4) Deleted

2-4.3.8 Missing Files or Serials (See MIOG, Part 2, 26-13.2.)

(1) Files or serials missing for 30 days are to be reported to the Information Resources Division, Attention: Information Management Section.

(a) In the event these files or serials contain classified material, the aforementioned information must be accompanied by a damage assessment, as outlined in the Manual of Investigative Operations and Guidelines, Part 2, Section 26-13.1. The damage assessment will be forwarded to the Security Programs Manager (SPM), FBIHQ.

(b) When files and serials are located, information concerning the circumstances of the recovery is to be furnished to FBIHQ.

(c) If the files or serials are classified, efforts should be directed to identify individuals having possession, and if these individuals possess appropriate security clearance and "need-to- know" access to the files or serials. If the individuals do not possess appropriate security clearances and "need-to-know" access, they are to be interviewed regarding the circumstances surrounding their exposure to the information and be given the FD-722, "Inadvertent Disclosure Statement," in accordance with current procedures in the Manual of Investigative Operations and Guidelines, Part 2, Section 26-4.1.

(2) On 60-day intervals, the Administrative Officer (AO)/ Office Services Manager (OSM) is to direct to the SAC a communication advising SAC of the status of missing material and efforts to locate same (communication not to be furnished to FBIHQ). Such communications are to be reviewed and initialed by the SAC for subsequent filing in the control file. On December 1st of each year, the AO/OSM will again direct to the SAC a communication recapitulating all missing material and indicating what efforts are being made to locate same. After this communication has been reviewed and the SAC is satisfied that sound procedures to facilitate locating missing material have been implemented and are being adhered to, SAC should initial the communication for subsequent filing in the control file (communication not to be furnished to FBIHQ). All 60-day follow-up communications that have been incorporated into the December 1st communication are to be purged from the control file. The initial communication advising FBIHQ of the missing material is to be retained until files and/or serials are located, or destruction criteria have been met.

(3) It will be the responsibility of each SAC to follow this matter to ensure that every effort is being made to recover material that is missing. FBIHQ does not intend to follow with any office regarding this matter but will collect this information for accountability and statistical purposes only to later be incorporated into a profile report and furnished to the Inspection Staff for their scrutiny and evaluation at the time the respective field office is inspected. Should it be determined that files and/or serials are missing as a result of employee negligence or willful destruction of such material, it will be the responsibility of the SAC to notify and make appropriate recommendations to the Office of Professional Responsibility.

2-4.4 Retention of Property by the FBI

2-4.4.1 Evidence (See MAOP, Part II, 6-13.9(6).)

(1) Property may be acquired during investigations in accordance with the law concerning searches and seizures, and by warrant, subpoena, or consent including voluntary delivery. If a request is made by anyone that property is to be taken into possession in any other manner, employees must explain their lack of authority. Form FD-597 (Receipt for Property Received/Returned/Released/Seized) is to be used to document the receipt/return of property acquired during investigations. The FD-597 consists of an original and two copies with carbon insert. The original is to be filed in the 1A section (FD-340a) of the investigative case file. One copy of the FD- 597 is to be furnished to the contributor, and one copy, when appropriate, returned with the search warrant.

(2) It is essential that seized/recovered/contributed property be properly identified and described by investigative personnel at the time possession is transferred to the investigator. The items are to be carefully packaged and the containers properly identified. If appropriate, chain of custody is to be established and a record thereof is to be maintained from the time possession transfers to the investigator to the time of trial/disposition. To minimize the number of FBI personnel required to establish chain of custody, it is recommended that one or two investigators be designated to identify and describe all evidence at any particular search or arrest site.

2-4.4.2 Evidence Control Room (ECR) (See MAOP, Part II, 2-4.4.4 and 2-4.4.10.)

(1) The designated ECR should be a separate area, usually within the confines of field office space, used solely for the storage of seized/recovered/contributed property which can reasonably be expected to be introduced in court and/or subject to chain of custody, regardless of size. Access to the ECR is restricted to ensure evidentiary property is accounted for, retrievable, and can withstand defense challenges concerning chain of custody.

(a) [redacted] b2

(b) Appropriate personal protective supplies and first aid and safety equipment should be stored in the ECR for easy accessibility. This includes, but is not limited to: disposable gloves/gowns, disposable plastic aprons, eye/mouth protection, pails with disinfectant, biohazard bags for disposing biohazard material (bag to be placed in a hard cardboard box), containers to hold needles, sink with hot and cold running water (with elbow or foot connection), flammable cabinets, acid cabinets, poison cabinets, and biohazard labels and containers.

(c) The Drug Vault (or room) should be afforded outside ventilation for the storage of odoriferous substances. The floor should be made of a nonporous material so that it can be disinfected.

(d) In the event evidentiary property is of such volume that it is not practical to store in the ECR or similar facility within field office space, it may be stored in a secure off-site facility at the discretion of the Special Agent in Charge (SAC). The off-site facility should be established in accordance with the guidelines set forth in (1) (a) through (c) above. Every effort should be made to store evidence in the ECR; however, if a similar facility within field office space or an off-site facility is used, these facilities are considered satellites of the ECR and are subject to the same administrative controls afforded the ECR.

(2) Form FD-455 (Access Log - Evidence Storage Facility) is to be maintained for each ECR or satellite ECR whether located within field office space or an off-site. In addition, a separate FD-455 is to be maintained for each valuable, drug, and ELSUR evidence repository regardless of size or location. The FD-455 establishes a reliable record of persons gaining entry. The visitor SIGNS his/her own name - one name per line, reason for entry, the case file number and 1B/1D serial number, if appropriate, and the date and time of entry/exit. This information is extremely useful in defense against attacks regarding chain of custody. In field offices where an "enclosed reception area" has been established at the entrance to the ECR, it is not required that the FD-455 be signed as long as the visitor does not enter beyond this "enclosed reception area." Investigative personnel reviewing evidence in the "enclosed reception area" are not required to sign the FD-455; however, the chain of custody must be signed as a record of their review of the evidence. The FD-455 logs are to be maintained from inspection to inspection. The logs are eligible for destruction following an inspection when the evidence, pertaining to the log entries, has been disposed of or the files listed on the log are eligible for destruction, whichever is sooner. (See 2-4.4.7 (1).)

(a) The Evidence Control Technician (ECT) and Alternate Evidence Control Technician (AECT), when substituting for the ECT for one day or longer, are required to sign in and out on the FD-455 log maintained for the ECR only upon initial entry and final departure on a given day. Any other employee, including the AECT, when the ECT is on duty, must sign in/out on the FD-455 log for each entry/exit on a given day. ONLY ONE SIGNATURE PER LINE IS PERMITTED.

(b) In those field offices where more than one full-time ECT and/or more than one evidence storage facility is operated on a daily basis, access to the storage facility(s) is to be recorded on the FD-455 log as follows:

The ECT must sign in/out on the FD-455 log for the primary ECR, when first entry/last exit of the day is made. Access to any satellite ECR must be recorded on the FD-455 log maintained for that satellite ECR for each entry/exit on a given day.

(3) Access to the ECR and/or other evidence storage facilities which store general evidence, located within or outside field office space, is strictly limited to the ECT and AECT(s). Access by other employees is prohibited unless accompanied by the ECT/AECT, or as outlined in (7) below, and documented on the FD-455 log maintained for the facility accessed.

(4) In instances involving large seizures of evidentiary property which occur during off-duty hours (nights/weekends/ holidays), the services of the ECT/AECT should be used to assist with analyzing, cataloging, inventory and storage of the seized/recovered property.

(5) In the event that the services of ECT/AECT are not utilized, a secured night depository is to be used for the temporary storage of valuable/drug evidence until the next business day. The night depository should be secured to the floor either outside the ECR or in the Night Supervisor's working area.

(6) The ECT/AECT is not authorized to access the Drug/Valuable Vault unless accompanied by the Administrative Officer (AO) or the person(s) designated to act on behalf of the AO as the Vault Witness Official (VWO). The vault witness responsibility remains with the AO, but the actual duty may be delegated to meet the requirements of the field office and resident agencies. However, the VWO should not be an AECT. Each office should limit the number of designated VWOs, and must document the list of authorized vault witnessing personnel in the evidence control file. The VWO must also sign the FD-455 for each entry/exit.

(7) The only persons having emergency access to the Drug/Valuable Vault (both combinations or both keys) and the ECR will be the Special Agent in Charge (SAC), the Assistant Special Agent(s) in Charge (ASAC), and the Supervisory Special Resident Agent (SSRA). The written access numbers to the combination(s) or the key(s) for the dual access entry must be stored separately. One combination (or key) is to be maintained in a GSA-approved security container with the central combination record file; the other combination (or key) is to be placed in the COMSEC vault safe. The SAC/ASAC/SSRA who makes an emergency entry/exit into the ECR must sign the FD-455, and document their access by an electronic communication (EC) to the Evidence Control File. (See (3).)

(8) A refrigerator/freezer is to be placed in the ECR for the storage of body fluids and any perishable-type evidence. Food items, for personal consumption, are NOT to be stored in this refrigerator.

(9) On the entrance to the ECR (preferably the door) and on the refrigerator in the ECR, a BIOHAZARD WARNING label is to be placed.

2-4.4.3 Responsibilities of the Evidence Control Technician (ECT) (See MAOP, Part 2, 2-4.4.10.)

The ECT is designated custodian of seized/recovered evidentiary property which encompasses the following responsibilities:

(1) Familiarity with the procedures set forth herein; the Manual of Investigative Operations and Guidelines (MIOG), Part 2, Section 13 (Laboratory Division Aids to Investigations) for assistance in the collection, identification, preservation, packaging and transmittal of evidence; HANDBOOK OF FORENSIC SCIENCE; MIOG, Part 2, 13-6.7.1 concerning the handling and storage of hazardous chemicals; the Forfeiture Manual concerning the disposition of property subject to forfeiture and the Forfeiture and Abandoned Property Manual, Section 10, concerning Dangerous Goods Regulations, International Air Transport Association (IATA).

(2) Ensures that access to the Evidence Control Room (ECR) and other evidence storage facilities is limited to persons having an official need; that all individuals entering the facilities are escorted and that access is recorded on Form FD-455 (Access Log - Evidence Storage Facility) maintained for EACH storage facility.

(3) Ensures that the proper protective clothing/equipment is stored and is readily available in the ECR, and is utilized when handling hazardous or potentially hazardous evidentiary property.

(4) In conjunction with Subpart H of Title 49, Code of Federal Regulations, Part 172 which requires that training be provided to those individuals who, in the course of their employment, directly affect Hazardous Materials (HAZMAT) transportation safety, the ECT is to avail himself/herself of such training. ECTs are to receive specialized HAZMAT training for air transport shipments every two years by a certified Department of Transportation or IATA-approved school. Strict fines are imposed on individual employees by the Federal Aviation Administration for noncompliance.

(5) Ensures, by physical examination of property, that the descriptive data entered into the automated evidence system (aka "Collected Item"), as furnished by case Agent/acquiring Agent, adequately reflects the property to be retained. (When evidence is heat-sealed, the sealing/witnessing officials are responsible for the accurate description of the evidentiary items.)

(6) Responsible for the recordkeeping, storage, and maintenance of all evidence. Responsibility for nonevidentiary property acquired during investigations may, at the discretion of the SAC, be assigned to the ECT if his/her workload permits. Otherwise, the SAC should assign responsibility for nonevidentiary property to an employee other than the ECT.

(7) The case Agent, acquiring Agent, and/or Agent Supervisor, depending upon the circumstances, as individuals or collectively, share the responsibility for ensuring that seized/recovered/contributed evidence is properly documented on the FD-192. The evidence and/or documentation is to be submitted to the ECT within 10 calendar days from the date that the evidence was seized/recovered. Should extenuating circumstances prevent handling of the evidence within 10 calendar days, the ECT advises the Agent that an electronic communication (EC), aka Late Day Memo, is to be submitted to the SAC, signed by the Squad Supervisor and thereafter placed in the investigative case file. (A copy of the EC is to be directed to the ECT, placed in a binder in the ECR, and maintained from inspection to inspection.) The ECT is authorized to reject evidence that is submitted late without the accompaniment of an EC. The 10 calendar days for the acquiring Agent begin with the seizure of the property and end when the ECT receives the evidence and signs the chain of custody. (If the acquiring Agent submits only the FD-192, thereby maintaining the evidence, the ECT is to be cognizant of the 10-day time frame and should not accept the late FD-192 without an EC. In the event the evidence is retained by the acquiring Agent, proper charge-out procedures are to be followed.)

(a) When lead offices (LOs) forward evidence to the office of origin (OO), the following documents (when necessary) should accompany the evidence:

FD-192 (package copy and file copy) EC for late submission - SA and/or ECT FD-597

(See also 2-4.4.4 (2).)

(8) The ECT is responsible for ensuring that the seized/recovered/contributed evidence is properly captured in Collected Item within 10 calendar days from the date the evidence and/or documentation was presented to him/her by the seizing Agent. Should extenuating circumstances prevent the ECT from entering the information into the automated evidence system, aka Collected

Item, within 10 calendar days, the AO is to be advised by EC which is to be placed in the investigative case file. (A copy of the ECT's EC is placed in a binder in the ECR, and maintained from inspection to inspection.) The 10 calendar days for the ECT begin when:

(a) he/she signs the chain of custody at the time he/she acquires the evidence, or

(b) when he/she acquires only the documentation, and ends when he/she enters the information into Collected Item. (See 2-4.4.4 (3).)

(9) Ensures that exact location of property is noted in Collected Item; that the 1B, 1C, or 1D serial number is recorded on the automated FD-192/FD-192a for file; that bar code labels are placed directly on the general evidence packaging, and on the plastic pouches containing valuable or drug evidence; that an automated FD-192/FD-192a is filed in the case file and a second copy is attached to the property or placed in the binder/folder maintained in the valuable/drug evidence repository.

(10) Ensures chain of custody documentation for evidence is recorded in Collected Item and on the automated FD-192 maintained with the evidence.

(11) Ensures evidence is properly packaged and labeled for forwarding to FBIHQ other field offices, Drug Enforcement Agency (DEA), or contributor and that transmittal/disposition information is recorded in Collected Item.

(12) Retrieves evidence from the ECR and any other evidence storage facility as requested by Agent personnel; accurately records chain of custody on the form maintained with the package copy of the automated FD-192; and in Collected Item; produces a charge-out reminder report to ensure property held over 60 days is either recharged or returned to the storage facility.

(13) Upon request, retrieves nonevidentiary property from the facility and charges out the property by using an FD-5 (Charge- Out form) in accordance with established charge-out procedures. Maintains and monitors a record of property charged out to ensure nonevidentiary property held over 60 days is either recharged or returned to the facility.

(14) Follows closely the automated property disposition tracking system to ensure every effort is made to return property to contributor and/or property declared abandoned is processed on a timely basis. Closed Cases with Pending Evidence Report is to be run and distributed to squad supervisor(s) for evidence disposition decisions every 60 days.

(15) Disposes of property on instructions of FBIHQ, other field offices, or Agent personnel through actual destruction (drug evidence excluded), return to contributor, or other methods as appropriate. Should property that has been declared abandoned become the property of the FBI, ensures action is taken by supply personnel to have the property placed on the field office inventory.

(16) As necessary, may be required to testify in a court of law regarding evidentiary property (chain of custody) for which responsible.

(17) At the discretion of the SAC, serves as a fully trained member of the Evidence Response Team.

(18) Upon the advice of the Evidence Program Manager, FBIHQ, and at the request of the Inspection Division, FBIHQ, conducts inspections of field office evidence programs with SAC approval.

(19) At the request of the Evidence Program Manager, FBIHQ, and with the consent of the SAC, assists the Evidence Program Manager to conduct training and ECR assessments in various field offices.

2-4.4.4 Evidentiary Property (See MAOP, Part 2, 2-4.4.11 (3) and 2-4.4.16.)

To facilitate recordkeeping and storage procedures, evidentiary property is divided into three categories: general evidence, valuable evidence, and drug evidence. All newly acquired evidence must be entered into Collected Item.

Procedures for the administrative handling and storage of evidence are as follows:

(1) In field offices where Special Agent personnel do not directly enter their own evidence into Collected Item, the traditional green FD-192 is to be used as a "data loading form" (draft) to communicate to the ECT the information that is to be entered in Collected Item. The evidence, together with the "draft" FD-192, a signed chain of custody (automated sheet), and the case file, are then furnished to the ECT. Upon entering the information into Collected Item, the "draft" FD-192 is thereafter destroyed. It is NOT to be used as the file or package copy. (See (11).)

(2) The evidence and/or the documentation is to be submitted to the ECT within 10 calendar days from the date the evidence was seized/recovered/contributed. Should extenuating circumstances prevent handling of the evidence within 10 calendar days, the ECT advises the SA that an EC (aka Late Day Memo), is to be submitted to the SAC, signed by the Squad Supervisor and thereafter placed in the investigative case file. (A copy of the EC is to be directed to the ECT, placed in a binder in the ECR, and maintained from inspection to inspection.) The ECT is authorized to reject evidence that is submitted late without the accompaniment of an EC. The 10 calendar days for the acquiring Agent begin with the seizure of the property and ends when the ECT receives the evidence and signs the chain of custody. (If the acquiring Agent submits only the FD-192, thereby maintaining the evidence, the ECT is to be cognizant of the 10-day time frame and should not accept the late FD-192 without an EC. In the event the evidence is retained by the acquiring Agent, proper charge-out procedures are to be followed.)

(a) When LOs forward evidence to the OO, the following documents (when necessary) should accompany the evidence:

FD-192 (package copy and file copy) EC for late submission - SA and/or ECT FD-597

(See also 2-4.4.3 (7).)

(3) In field offices where Agent personnel directly enter their own evidence into Collected Item, the Agent sends the automated FD-192 to the ECT's printer and thereafter provides the evidence, together with a signed chain of custody (automated sheet), and the case file to the ECT. The 10 calendar days for the acquiring Agent begin with the seizure of the property and end when the ECT receives the entered information through Collected Item.

(4) The ECT is responsible for ensuring that the seized/recovered/contributed evidence is properly captured in Collected Item within 10 calendar days from the date the evidence and/or documentation was presented to him/her by the seizing Agent. Should extenuating circumstances prevent the ECT from entering the information into Collected Item within 10 calendar days, the AO

is to be advised by an EC which is to be placed in the investigative case file. (A copy of the ECT's EC is placed in a binder in the ECR, and maintained from inspection to inspection.) The 10 calendar days for the ECT begin when:

(a) he/she signs the chain of custody at the time he/she acquires the evidence

(b) when he/she acquires only the documentation, and ends when he/she enters the information into Collected Item. (See 2-4.4.3 (8).)

(5) The ECT accepts the evidence and signs the chain of custody. He/She then enters the required information (if not already done so by the Agent), and produces a bar code number (which is affixed to the evidence packaging) and a 1B/1D serial number. (For detailed procedures on entering evidence into Collected Item, see the AUTOMATED CASE SUPPORT (ACS) USERS' GUIDE.) The chain of custody and a record thereof must be maintained on evidentiary items from the time of acquisition to the time of disposition.

(6) Upon assigning the bar code to the evidence, the ECT is required to print three new copies of the FD-192 which show the bar code. One copy of the automated FD-192 (file copy) is submitted to the Supervisory Special Agent (SSA), primary relief supervisor, ASAC or SAC for initialing, and is then filed in the first section of the investigative case file immediately above the 1A section (FD-340a). (See (11)(c).) If there is no 1A section, the file copy becomes the first item in the first section of the investigative case file. The file copy may be maintained in a subfile, in which case a blank automated FD-192 should be placed in the main file as a substitute for the original indicating their location, i.e., "1B serials maintained in Subfile E."

(7) For GENERAL EVIDENCE, the second copy (package copy) of the automated FD-192 and the written chain of custody is affixed to and remains with the evidence until final disposition. For VALUABLE AND DRUG EVIDENCE, the package copy and the written chain of custody is filed in numerical sequence, by file number, in a binder which is maintained in the ECR.

(8) The third copy is an informational copy which is to be forwarded to the paralegal specialist within the field office for forfeiture potential. (See (11).)

(9) The written chain of custody documents the SIGNATURES of persons, including the ECT, who receive custody of the evidence while it is the property of the FBI. The first chain of custody is established as a result of entering the group data on the first page of the automated FD-192 and indicates the identity of the person who collected the evidence. Subsequent chain-of-custody signatures will be made by the ECT or other individuals who receive the property. Chain-of-custody entries should not disclose that the evidence is received by the ECR; instead the entry should show the signature of the person to whom the custody of the evidence has been given. (The only exception to this policy is when evidence is forwarded to the DEA or FBI Laboratories.)

(10) In task force investigations, it is permissible for a federal criminal investigative agent from a participating federal agency or a deputized officer from a participating police department, to record chain of custody on Form FD-192 (Control Form for General/Valuable/Drug Evidence) when that investigator/officer is involved in the acquisition of the property documented on the FD-192. He/She may also participate as the sealing/witnessing agent in the verification and sealing of

DRUG/VALUABLE EVIDENCE. Support employees may be witnessing officials for valuable evidence only.

(11) In EMERGENCY SITUATIONS where circumstances dictate the immediate transmittal of evidence to FBIHQ and/or the DEA Laboratory by Agent personnel in an RA, prior to being furnished to the ECT for handling, the property must be documented, within the 10- calendar-day time frame, in Collected Item as noted in Section 2-4.4.4 (1) through (8), and handled according to the following procedures:

(a) The case/seizing Agent is to note transmittal information on the chain-of-custody page of the automated FD-192, (i.e., forwarded to FBI/DEA Lab, registered mail number or Federal Express number, date of transmittal letter, etc.), and furnish the chain of custody and an automated FD-192 (or a drafted green data- loading FD-192) to the ECT. The ECT does NOT sign the chain-of-custody page unless he/she is physically taking custody of the evidence; however, the appropriate information must be recorded in Collected Item. (See (21)(d).)

(b) The ECT assigns a bar code number and a 1B serial number to the evidence documentation. The bar code label is held by the ECT until the evidence is returned by the DEA or FBI Laboratory.

(c) The file copy of the automated FD-192 is initialed by an SSA and filed in the case file as noted in Section 2-4.4.4 (6).

(d) The package copy of the automated FD-192 is retained in the ECR and filed in a binder labeled "Evidence sent to FBIHQ" or "Evidence sent to DEA Lab" according to the transmittal date.

(e) When the evidence is returned to the field office, the ECT attaches the assigned bar code to the property, and properly executes the chain of custody on the package copy of the automated FD-192. The package copy of the automated FD-192 is affixed to the general evidence or filed in the binder maintained in the valuable/drug vault. The chain-of-custody information is then entered into Collected Item.

(f) If the evidence is to be returned to the RA, and not to the ECT in Headquarters City, the RA is to request that a copy of the laboratory report be furnished to the ECT when the evidence is returned to the RA.

(12) Collected Item will produce 60-day charge-out reminders.

(13) Property or items seized or recovered incidental to a search and seizure should generally be treated as evidence and maintained in the ECR. The below-listed material/items, are currently considered hazardous materials.

Flash Paper Live Ammunition Explosives Radioactive Materials Flammable Liquids and Solids Flammable and Nonflammable Gases Spontaneously Combustible Substances Oxidizing and Corrosive Materials

All require special packaging and the amount of each item which can be shipped is regulated. (See the Manual of Investigative Operations and Guidelines (MIOG), Part 2, 13-6.7.1 and the HANDBOOK OF FORENSIC SCIENCE for specific requirements and instructions for the handling/storing/shipping hazardous materials.)

(14) Property seized for forfeiture, which is also evidence, should be treated as evidence and maintained in the ECR during the forfeiture process. (See the Forfeiture Manual, Step 3-1.)

(15) Nonevidentiary property, if size permits, may be filed in the 1A section of the case file. Otherwise, large nonevidentiary property (serialized as a 1C), seized, subpoenaed or contributed pursuant to investigative activity, is to be stored in a separate area within, or, at the discretion of the SAC, outside the field office, in space specifically designated for the storage of nonevidentiary items. (See 2-4.4.16.)

(16) Chain of custody on Grand Jury Material (Rule 6E Material) is not required unless specified by the case Agent. The case Agent will consult with the AUSA to determine whether chain of custody should be maintained on specific Grand Jury Material. If so required, an FD-192 is completed and the material is stored in the ECR. When a chain of custody is not required, Grand Jury Material is documented on Form FD-192a (Control Form for Nonevidentiary Items), entered into Collected Item as a 1C serial, and segregated from the other nonevidentiary property, with access given only to those individuals named on the Grand Jury List. When Grand Jury Material is entered into Collected Item as a 1C, it is charged out by using Form FD-5 (Serial Charge-Out). (See MAOP, Part 2, 2-4.4.16 and 10-13.8 and MIOG, Part 2, 2-9.5 and 2-9.7.)

(17) Special Agents' original interview notes are not intended to be used as evidence at a trial, and questions raised by the defense with respect to them generally attempt to focus on inconsistencies between the original notes and the resulting FD-302. Just as it is not necessary to maintain chain of custody on the FD-302, it is not necessary to maintain chain of custody on original interview notes and they should be filed in the 1A section (FD-340a) of the case file.

(18) Classified National Security Information should be handled in the same manner as other evidence, with the exception that it must be retained in a storage receptacle, appropriate to its level of classification, with full consideration as to the necessary chain-of-custody accountability. Money, weapons, and other items of intrinsic value shall not be stored in the same security container unless they are also classified. Material believed to be classified, but not so identified, must be protected as though it is classified. Within 30 days a determination as to its classification must be made either by presentation of the material to an Original Classification Authority or comparison with an approved classification guide in accordance with MIOG, Part 2, 26-2.3. Under no circumstances will classified material be released to any person unless it has been determined that they have the necessary clearance and/or access commensurate with the classification level of the material and a demonstrated need to know.

(19) Electronic Surveillance (ELSUR) evidence (serialized as a 1D) should be handled in the same manner as general evidence, with the exception of Title III material which must be sealed within five (5) days by the court. (See MIOG, Part 2, 10-9.) However, ELSUR evidence is not to be stored in the ECR, but rather in a room specifically designated for such material. The physical requirements for this room are the same as for an ECR (see 2-4.4.2). (See FCI Manual, Introduction, 1-2.6.3.)

(20) Obscene material which will be retained as evidence must be clearly marked "Obscene" and stored as general evidence in the Evidence Control Room (ECR). (See 2-4.4.11 and MIOG, Part 1, 145-2; Correspondence Guide - Field, 1-14.)

(21) For Preautomated Evidence only:

Every effort should be made to enter all evidence into Collected Item. However, if extenuating circumstances prevent the entry of preautomated evidence into Collected Item, the following guidelines are to be followed:

(a) Three copies of the nonautomated green Form FD-192 should exist for preautomated evidence.

1. The original copy must be signed by an SSA and filed in the first section of the case file immediately above the 1A section (FD-340a). If there is no 1A section, the file copy becomes the first item in the first section of the case file. The file copy may be maintained in a subfile, in which case a blank nonautomated green FD-192 should be placed in the main file as a substitute for the original indicating their location, i.e., "1B serials maintained in Subfile E."

2. The package copy of the nonautomated green FD-192 records the chain of custody and must remain with general evidence. (If valuable/drug evidence, the package copy is not affixed to the property, but is filed in numerical sequence by file number in a binder which is maintained in the valuable/drug evidence repository. The package copy may be reproduced if more than one copy is required.) The signatures of persons, including the ECT, accepting custody must be recorded thereon as follows:

a. The first chain-of-custody entry is the employee who first acquired the property as identified on the front page of the nonautomated green FD-192.

b. The second chain-of-custody entry is the individual to whom the property was first released. The date, time and reason for release is also required.

c. The third chain-of-custody entry is the signature of the ECT or other individual who accepts possession from the individual releasing it (second chain-of-custody entry) along with the date, time, and reason for acceptance.

d. Chain-of-custody information continues in this fashion as the property changes hands. Chain-of-custody entries should not disclose that the evidence is released to or accepted by the ECR; the entry must show the signature of the person accepting/releasing custody.

3. It is the responsibility of the ECT to ensure that the chain of custody is accurately recorded on the package copy of the nonautomated green FD-192.

4. The index copy of the nonautomated green FD-192 serves as the index of property acquired as evidence. A consolidated record of all index copies is to be maintained in the ECR in a binder labeled "(Name of Field Office) - Index of Evidence." The index copies are to be filed by evidence category (general, valuable, drug) in numerical sequence by file number. If a satellite ECR is established in a resident agency (RA), the index copies of the nonautomated green FD-192s for evidence maintained in that RA are to be maintained in the field office Headquarters City ECR in a separate binder labeled "(Name of Resident Agency) - Index of Evidence" and filed therein as noted above. To maintain an effective recordkeeping system and to facilitate the conduct of physical inventories as required in Section 2-4.4.15, the Headquarters City's and RA's indexes must be kept up to date by noting any type of chargeout/transmittal/ disposition of property on the appropriate index copy.

(b) A 1B number should be assigned to the nonautomated green FD-192 by the ECT. A notation should be made on the nonautomated green FD-192 noting the exact location of the property stored in the ECR. When applicable, the 1B number should also be listed on the evidence label attached to the plastic pouch containing drug or valuable evidence. The ECT should ensure that the location of the property and the 1B serial number are legible on each copy of the nonautomated green FD-192.

(c) When physical inventories are conducted as required in Section 2-4.4.15, the inventories of preautomated evidence will be reconciled with the index copies of the nonautomated green FD-192s maintained by the ECT in the Headquarters City ECR, not those maintained in satellite ECRs in the RA. Therefore, the Headquarters City ECT should be advised of any type chargeout/transmittal/disposition of property located in the RA to prevent discrepancies.

(d) If preautomated evidence is required to be transmitted to FBIHQ and/or the DEA Laboratory, it is suggested that the evidence be immediately entered into Collected Item, and handled according to the guidelines as noted in Section 2-4.4.4 (11)(a).

2-4.4.5 General Evidence

(1) Items of evidence such as firearms, ammunition, clothing, typewriters, computer equipment, latent fingerprints lifted from a crime scene, and documentary items (exclusive of ELSUR evidence) such as books of account, printed materials, video tapes, motion picture films, magnetically or electronically recorded cards, tapes, discs, are treated as general evidence and stored within the ECR.

(2) If documentary items have been admitted into evidence during court proceedings or serve a continuing law enforcement purpose, the items may be retained by the FBI with the concurrence of the USA. (See also MIOG, Part II, Section 28 and Legal Handbook for Special Agents, 5-12.4.)

(3) ELSUR evidence is treated as general evidence in Collected Item, and handled in accordance with procedures set forth herein, and in MIOG, Part II, 10-9.

(4) Clothing that may contain blood and/or other liquids of known or unknown origin, should be completely dried before being stored or shipped. In field offices that are moving to newly acquired space, or being renovated, a separate room (not inhabited by employees) should be utilized to air-dry these garments. This room is to be either in the ECR or adjacent to the ECR and have outside ventilation. If the drying room is outside of the ECR, it must be as secure as the ECR.

(5) Prior to storing and/or shipping blood-stained garments, the HANDBOOK OF FORENSIC SCIENCE and the DANGEROUS GOODS REGULATIONS should be consulted.

2-4.4.6 Firearms (Moved from 2-4.4.3) (See 2-4.4.17.)

(1) By Statutes

(a) Title 18, USC, Section 3665, provides as follows: Firearms possessed by convicted felons-

"A judgment of conviction for transporting a stolen motor vehicle in interstate or foreign commerce or for committing or attempting to commit a felony in violation of any law of the United States involving the use of threats, force, or violence or perpetrated in whole or in part by the use of firearms, may, in addition to the penalty provided by law for such offense, order the confiscation

and disposal of firearms and ammunition found in the possession or under the immediate control of the defendant at the time of his arrest. The court may direct the delivery of such firearms or ammunition to the law-enforcement agency which apprehended such person, for its use or for any other disposition in its discretion."

(b) In all cases in which firearms and ammunition are seized pursuant to the above statute, the USA shall be notified of the seizure so that USA may bring it to the attention of the court at the time of sentencing.

(c) There is no objection to a court order directing disposal by the FBI Laboratory. (See MIOG, Part II, 13-12.8.)

(d) Other federal statutes, indexed under "Firearms" in the U.S. Code Annotated, provide for forfeiture of firearms used in violation of various statutes including liquor laws and used in named national parks and declaring contraband any firearm with respect to which there has been committed a violation of any provision of the National Firearms Act or any regulation issued pursuant thereto. The responsibility for selecting the applicable statutes, if any, is that of the USA.

(2) By Other Means - If Title 18, USC, Section 3665, or other statutes relating to confiscation or forfeiture do not apply, the firearms shall be disposed of as follows:

(a) If the firearm is the property of the subject, obtain from subject a signed waiver of ownership rights and forward the firearm to the FBI Laboratory.

(b) If the firearm is the property of the subject and subject is convicted and will not waive ownership rights, deliver the firearm to the USM as part of subject's property or deliver it to subject's attorney or other designated representatives.

(c) If the firearm is the property of the subject and subject is acquitted and will not waive ownership rights, deliver the firearm to subject or to designated representative.

(d) If the firearm was stolen from a known and legitimate owner, return the firearm to owner. If the firearm is the property of the United States, return it to the nearest appropriate government agency office.

(e) If the legitimate owner of the firearm cannot be determined, deliver the firearm to the USM as abandoned or unclaimed property unless the firearm bears a U.S. government stamp in which case it should be determined if it is desired for inclusion in the Reference Firearms Collection (RFC) of the FBI Laboratory and, if not, it should be forwarded by express, collect, to the nearest U.S. Army Ordnance arsenal or depot with the request that a receipt be furnished the field office by the military authorities.

(f) Whatever the ownership status of the firearm, if the Bureau only borrowed it as evidence from another law enforcement agency which obtained it upon arrest of the subject, it should be returned to that agency.

(g) If the subject is not prosecuted federally and is delivered to some other agency, as in the case of a deserter or a person arrested for unlawful flight to avoid prosecution, deliver the firearm to that agency, along with the subject.

(3) In situations (b) through (g) above, obtain a receipt (FD-597) from person to whom firearm is delivered and place it in the 1A section of the investigative case file.

(4) If a firearm (or ammunition) is held for evidence and any person demands the immediate return of it, or a firearm is otherwise held and two or more claimants dispute ownership, hold the weapon and refer the legal problem to the USA.

(5) Any offer of a firearm for inclusion in the RFC should be accepted only if the owner will furnish a release showing that the weapon is being given to the FBI unconditionally with the understanding that if the FBI Laboratory has a similar weapon or for any other reason does not desire its retention, the weapon may be destroyed.

(6) All firearms obtained by the FBI through a court order or waiver of ownership shall be handled according to the following criteria:

(a) All firearms shall be submitted to the Firearms- Toolmarks Unit, FBI Laboratory, along with any requests for their return to the field offices and justification for such action.

(b) The Laboratory shall have the option of retaining any such firearms for its RFC unless specifically instructed by court order to destroy a firearm.

(c) The FBI Academy, Quantico, will be advised by the Laboratory of any firearms received that are not being included in the RFC and will decide whether they are needed for training purposes or for reissue.

(d) If there is a request for the return of the firearm to the field office for issue or display and if it is not needed by the Laboratory or Training Division, the Training Division will evaluate the request and, if approved, will perform the necessary refurbishing, or deactivation of these firearms. It is to be noted that approval of such requests will not be routine and must be supported by ample justification.

(e) If not needed by the Training or Laboratory Division and there is no request to return the firearm to the field (or if request denied), the Laboratory will destroy the firearm. The field office is not authorized to destroy any confiscated firearms.

(7) Seized/recovered firearms that are to be retained by FBI field offices pending resolution of an investigative matter are to be stored in the Evidence Control Room (ECR).

(8) Firearms are not to be accepted by the ECT for storage until they have been examined by a field office Firearms Instructor and rendered safe. THE FIREARMS INSTRUCTOR IS TO CERTIFY THE EXAMINATION BY:

(a) SIGNING HIS/HER NAME, AND

(b) PLACING THE DATE THAT THE WEAPON WAS EXAMINED AND RENDERED SAFE IN THE LOWER LEFT HAND CORNER OF THE CHAIN-OF- CUSTODY PAGE OF THE PACKAGE COPY OF THE AUTOMATED FD-192.

Chain-of-custody information is not to be recorded if possession of the firearm does not change during the safety examination. Once rendered safe, firearms may be stored in a secured cabinet or on open shelving within the ECR.

2-4.4.7 Drug Evidence (See MAOP, Part II, 2-4.4.9, 2-4.4.10, 2-4.4.11; MIOG, Part I, 281-8.1 (3), 281-8.1.4 (2), 281-8.1.5, 281-8.1.6, 281-8.1.8, 281-8.1.12.)

(1) Drug evidence must be afforded maximum security while in the FBI's possession, and not co-mingled with any other type of evidence. Storage should be in one or more of the following types of facilities:

b2

(a)

(b)

Open-shelf filing is permissible in

(c)

Exterior ventilation for the storage of odoriferous substances and the health and safety of evidence personnel is to be afforded. Open shelving is permissible.

(d)

Exterior ventilation for the storage of odoriferous substances and the health and safety of evidence personnel is to be afforded.

Open shelving is permissible.

(e)

(f) A separate Form FD-455 (Access Log - Evidence Storage Facility) is to be maintained for EACH drug repository. If open shelving is utilized, then one FD-455 Log for the room/vault is sufficient. (See 2-4.4.2 (2).)

(g) The ECT/AECT is not authorized to access the drug/valuable storage facility unless accompanied by the AO, or the person(s) designated to act on behalf of the AO as the Vault

Witnessing Official (VWO). The vault witness responsibility remains with the AO, but the actual duty may be delegated to meet the requirements of the field office and resident agencies. However, the VWO should not be an AECT. Each office should limit the number of designated VWOs and must document the list of authorized vault witnessing personnel in the evidence control file.

(h) The Agent submitting the drug evidence to the ECT must remain with the ECT while he/she processes the evidentiary property and until the VWO arrives to access the vault and witness the storage of the drugs.

(i) The only persons having emergency access to the drug/valuable storage facility (both combinations or both keys) and the ECR will be the SAC, the ASAC, and the Supervisory Special Resident Agent. The written access numbers to the combination(s) (or the key(s) for the dual access entry to the drug/valuable vault) must be stored separately. One combination (or key) is to be maintained in a GSA-approved security container with the central combination record file; the other combination (or key) is to be placed in the COMSEC vault safe.

(2) Drug evidence should be stored in a reasonably controlled environment as elevated temperatures or humidity may result in some drug decomposition. Marijuana and crude preparations of some other drugs, such as cocaine, PCP and methamphetamine, are highly odoriferous and will require more than normal ventilation for odor control. Wet or freshly harvested marijuana will mildew if not thoroughly dried before being sealed and stored. It is also advisable to fumigate marijuana to curb insect growth within the bundles. For health and safety reasons, proper outside ventilation of the drug vault/room is required.

(3) Two federal criminal investigative agents and/or deputized officers (one designated the sealing agent/officer and one the witnessing agent/officer, who are not support employees) are responsible for ensuring that drug evidence is weighed/counted and verified before the evidence is sealed, transmitted to the DEA Laboratory or placed in storage in accordance with the following procedures:

(a) The drug evidence, along with the original container, is placed in an appropriate size plastic evidence pouch and weighed/counted. The weighing should be accomplished on a scale capable of weighing in gram increments and the weight recorded on the FD-723 (Evidence Label). If the drug seizure involves tablets or capsules, the number of tablets or capsules can be determined by actual count if the quantity is small or, if too voluminous to count, by computation based on relative weights, e.g., count and weigh 100 units to determine a unit weight and then divide this weight into the net weight of the entire exhibit to determine the total number of units. If liquids are involved, the gross quantity will be reported by volume. Estimates will be based on the known or apparent size of the container.

(b) The FD-723, is to be completed with the following information:

1. Field Office Name

2. File Number

3. Date of Seizure or Purchase

4. Sealing Official's Printed Name

5. Sealing Official's Signature

6. Witnessing Official's Printed Name

7. Witnessing Official's Signature

8. Laboratory Examiner's Signature

9. Weight (for drugs)

10. DEA Exhibit Number (for drugs)

(c) Ensure that the completed FD-723 is placed on the outside of the plastic evidence envelope, at the top, and folded at the perforation over both sides of the envelope. Insert the envelope into the heat sealer ensuring that the heat seal is made across the FD-723.

(d) The use of plastic evidence envelopes is not always practical for bulk drug evidence seizures. Therefore, the entire bulk shipment must be packaged in boxes or cartons of uniform size. Each box should contain no more than 15-20 kilograms of substance and should be packed as full as possible. Packing material should be added, if required, to ensure that boxes will not be crushed when stacked and transported.

1. Each box or carton is to be closed with fiber- reinforced plastic tape ensuring that the tape encircles the carton and that the tape ends meet or overlap on the top.

2. An FD-723 is to be completed to include the date of sealing and the printed names and signatures of the sealing agent/officer and witnessing agent/officer.

3. The FD-723 is to be affixed to each box at the top to ensure that it covers both ends of the plastic fiber- reinforced tape. The label should be covered with clear plastic tape to ensure that names and signatures are not obliterated during transport and handling.

4. Each box will be numbered consecutively (1 of 10; 2 of 10, 3 of 10, etc.) with a permanent marker in large print.

5. Each box should also be marked with the number of packages it contains. (For additional specifics on bulk drug seizures, see MIOG, Part I, 281-8.1 through 281-8.1.11.)

(e) Opening and resealing of drug evidence must be conducted in the presence of at least two federal criminal investigative agents/deputized officers. The reasons and procedures must be fully documented in an FD-302. Two copies of the FD-302 are to be generated - one is designated for the investigative case file, and a second copy is to be presented to the ECT with the resealed evidence. (The ECT is to maintain the ECR copy of the FD-302 in a binder from inspection to inspection).

(f) A sealed plastic evidence pouch is opened by cutting off the sealed upper edge with scissors or a paper cutter, ensuring that the FD-723 is intact. If the evidence is to be resealed, both portions of the used pouch are to be retained, placed in a new evidence pouch with the evidence and sealed following the above-mentioned instructions. Opening and resealing drug evidence is to be continued in this fashion.

(g) When bulk drug evidence is required to be opened, it is done so by first cutting the FD-723 from the top of the box. If the evidence is to be resealed, the previously used FD-723 is placed in a

plastic envelope inside the box, and the box is then sealed following the above-mentioned instructions. (For detailed procedures on entering drug evidence into Collected Item, see the ACS USERS GUIDE.)

(h) Investigative or operational requirements may necessitate the temporary storage of bulk drug evidence for later use by investigators. The original containers cannot be marked or otherwise altered without adversely affecting the investigation or operation. Storage of the drugs in the ECR is temporary, although the drugs may be permanently stored in the ECR at a later date. Under these circumstances, the drugs will remain in the original packaging (boxes, suitcases, individual kilograms, etc.) and will then be placed in additional boxes, cartons or other containers and sealed as described in paragraph (3)(d) above. The original packaging containing the drugs will not be marked or otherwise altered. In this manner, the original packaging containing the drugs remains unaltered, while the external packaging is sealed with appropriate documentation. (See MIOG, Part I, 281-8.1.12.)

(4) Laboratory analyses of seized drugs will be conducted by the DEA Laboratories. The transmittal to and return of drug evidence from the DEA Laboratories are to be recorded in Collected Item. (See MIOG, Part I, 281-8.1.3.)

(a) Usually, DEA is requested by the FBI to forward the original packaging that contained the drugs to the FBI Laboratory for latent fingerprint analysis. When this occurs, the packaging will be returned, separated from the drugs, and at a later date. To account for the evidentiary property that has now become two pieces, the "Split" function is performed in Collected Item when the drugs are returned. This will give both pieces of evidence their own chain of custody. If the drugs are properly sealed by the DEA chemist, the package is not to be resealed by the FBI, as the DEA chemist will testify to the contents and to his/her sealing procedures. (The DEA Laboratory may complete the lower portion of the FD-723 that states "for Lab use only." However, they are not required to do so, as DEA reseals the package with their own seal.)

(b) When drugs packaging has been examined for latent fingerprints by the FBI Laboratory (therefore having been separated from its original contents), it is also treated as a drug, and therefore should be sealed by the FBI Laboratory in the same manner as any drug. The FBI Laboratory will heat seal the packaging and complete the lower portion of the FD-723 that states "for Lab use only." The field office will process the sealed drugs packaging in Collected Item (continuing the entry that was began by the "Split" function), and place the evidence in storage in the drug vault.

(5) DEA Form 7 (Report of Drug Property Collected, Purchased or Seized) is a six-part form (original and five copies) and is to be utilized when transmitting drug evidence to the DEA Laboratory. DEA Form 7 is transmitted to the appropriate DEA Regional Laboratory by cover communication. Procedures for filling out the form are as follows:

(a) DEA Form 7 is to be typed. Each form is limited to three (3) exhibits inasmuch as there is not sufficient space for the results of analyses of more than three (3) exhibits. The submitting office case file number and exhibit number (see item 9) should be placed on all drug evidence pouches so they can be matched with the accompanying correspondence.

Item 1: Self-explanatory. Money flashed will be checked only where drugs were seized as a result of using a flash roll.

Item 2: Enter field office file number, e.g., 245A-HN-1234. This number is essential for future case identification and retrieval.

Item 3: Disregard.

Item 4: Enter "FBI."

Item 5: Self-explanatory.

Item 6: Disregard.

Item 7: Self-explanatory.

Item 8: Disregard.

Item 9: The exhibit number or sequence number is assigned by the submitting office or by the DEA chemist. An exhibit is defined as any substance differing in form, color or shape from any other submitted materials or acquired at a different time and place. When there are several submissions from one field office or separate submissions from several field offices, it will be the responsibility of the office of origin (OO) to assign the sequential exhibit numbers. The DEA Laboratory may also be contacted to determine the next sequential exhibit number for that particular case.

Item 10: The "alleged drug" is that drug which the evidence is purported to be, or is sold as, by the defendant.

Item 11: Describe fully the labels on the original containers and specify whether seals on these containers were intact. This entry may be continued under Item 15 ("Remarks"), as necessary.

Item 12: Approximate the amount of substance in each exhibit by size or weight. The exact count and precise weight of submitted exhibits will be determined by the DEA chemist.

Item 13: Indicate whether all the materials seized are being submitted or only a portion thereof.

Item 14: Complete only if the evidence was acquired through an undercover purchase.

Item 15: The OO and the OO file number must be identified under "Remarks." The OO file number will become the DEA Laboratory case control number for all future submissions in that case. When drug evidence is submitted by lead offices (LO), the LO must determine the OO file number and enter it under Item 15. Also, under "Remarks," it should be indicated whether latent fingerprint examinations or other forensic laboratory examinations are to be performed by the FBI's Laboratory Division. The cover communication should also set forth these requests and include appropriate case background data.

Item 16: Self-explanatory.

Item 17: Supervisory Special Agent.

(b) The copy distribution for DEA Form 7 is as follows:

Copies one through five are to be forwarded by cover communication, with the evidence, to the appropriate DEA Laboratory.

Copy six is to be detached by the submitting office and attached to the field office file copy of the cover communication and filed in the case file.

(c) Upon completion of the laboratory analyses, copy three will be sent to the OO and copies one and two will be returned to the submitting field office. These copies contain results of the DEA analyses and are to be filed in the 1A section (FD-340a) of the case file of the respective field office. All evidence will be returned to the submitting field office for retention and eventual destruction. The DEA Laboratory will not accept responsibility for the storage of drug evidence.

(6) The Federal-Wide Drug Seizure System (FDSS) is a computerized system which produces records of federal drug removals without regard for individual agency involvement. Participating agencies are DEA, FBI, the Immigration and Naturalization Service (INS), the U.S. Coast Guard (USCG), and the U.S. Customs Service (USCS). The FBI's participation in the FDSS is required whenever the weight of drugs recovered by the FBI exceeds established weight thresholds. At that time, a Federal Drug Identification Number (FDIN) will be telephonically obtained from the El Paso Intelligence Center (EPIC) and recorded on the DEA Form 7. The FDIN will be used by DEA's Statistical Services Section to capture records from the participating federal agencies. DEA's System to Retrieve Information from Drug Evidence (STRIDE) will continue to capture statistical information concerning FBI drug removals and will use that information for quality control of the FDSS. The following procedures have been established for implementation of the FDSS:

(a) An FDIN will be required for drugs recovered if the weight entered in Item #12 of DEA Form 7, "Approx. Gross Quantity Seized," or Item #13 of DEA Form 7, "Approx. Gross Quantity Submitted," exceeds the following thresholds:

Heroin 100 grams or 1/4 pound Morphine 100 grams or 1/4 pound Opium 500 grams or 1 pound Cocaine 500 grams or 1 pound Marijuana 25 kilograms or 50 pounds or 50 plants Khat 5 kilograms or 10 pounds Hashish 1 kilogram or 2 pounds LSD 100 units Other drugs 5,000 units

(b) Separate FDINs are required for each drug that exceeds the above weight thresholds, regardless of whether they came from the same incident. Samples extracted from a bulk seizure do not require separate FDINs.

Some examples of when an FDIN is needed are:

1. Exhibits 1, 2, and 3 of cocaine are seized during the execution of a warrant. Collectively the evidence weighs 900 grams; individually none weigh more than 500 grams. No FDIN is needed for any exhibit.

2. Exhibits 1, 2, and 3 of cocaine are seized during the execution of a warrant. Exhibit 1 weighs 600 grams and needs an FDIN. Exhibits 2 and 3 weigh less than 500 grams; neither requires an FDIN.

3. Exhibit 1 is 600 grams of cocaine. Exhibit 2 is 250 grams of heroin, and both were seized during the execution of a warrant. Each exhibit requires a separate FDIN.

4. Exhibit 1 is a bulk marijuana seizure, and is reported on DEA Form 7 along with sub-exhibits 1A through 1K which are samples extracted from the seizure. The total collected exceeds 25 kilograms. An FDIN is needed for exhibit 1, but not for sub-exhibits 1A through 1K.

(c) The FDIN will be obtained by the first federal agency to take custody of the drug evidence. On the rare occasions when the FBI assumes custody of drug evidence from another federal agency, the FDIN must be provided to the FBI as part of the custody transfer.

(d) Obtain the FDIN by contacting EPIC at FTS [redacted] or [redacted] Be ready to provide the following information, which will be recorded in a log maintained by EPIC: b2

1. Name and Title of Official Requesting the FDIN
2. Agency and Telephone Number of the Official Requesting the FDIN
3. Date and Local Time Collected
4. Place Collected (city, state)
5. Conveyance Type (e.g., vehicle, vessel, aircraft, or person)
6. Conveyance Identifier (e.g., name, number)
7. Quantity of Drug Collected (including unit of measure)
8. Type of Drug Collected (e.g., heroin, cocaine, or marijuana)

EPIC will issue an FDIN, which will be a ten-digit number beginning with the four digits of the fiscal year in which the drug evidence was collected, e.g., 1999000325. There will be no dashes or periods in the number.

(e) The FDIN is listed in the "Remarks" section of DEA Form 7.

(f) The method of drug removal (seized, recovered, collected, or purchased) does not affect the need for an FDIN. The determining factor is the weight estimate which includes the minimum wrapping necessary for evidentiary or packaging purposes. (See MIOG, Part I, 281-8.1.)

(8) To maintain the integrity of the drug evidence and to avoid unnecessary handling and possible exposure to toxic materials, Agent personnel should not attempt to transfer drug contents from the original package, wrapper or container into a substitute container. Those items which require both chemical analyses for drug contents and subsequent latent fingerprint or laboratory examinations of the packaging material itself for handwriting, or other type of forensic laboratory analyses, should be submitted to the DEA Laboratory and the appropriate information noted in the "Remarks" section of DEA Form 7. The DEA chemist will conduct the chemical analysis, then forward the items directly to FBIHQ, Attention: Laboratory Division, as appropriate.

(9) Drug evidence returned from DEA Laboratory is not to be opened, if properly sealed by the DEA chemist, but placed in storage as received. The DEA chemist occasionally removes the evidence from the original container(s) and returns the examined evidence to the submitting office in a substitute container(s) causing uncertainty as to whether the returned evidence is identical to the submitted evidence. In such instances, the ECT should note the change in containers on the package copy of the FD-192 stating the number of sealed containers returned from the DEA Laboratory and the DEA Laboratory numbers that appear on the containers and make appropriate modifications in Collected Item to accurately describe the evidence in storage.

2-4.4.8 Valuable Evidence (Moved from 2-4.4.6) (See MAOP, Part II, 2-4.4.9 and 2-4.4.10.)

(1) Valuable evidence is defined as money irrespective of amount and country of origin, jewelry irrespective of value and composition, negotiable documents, and other items of intrinsic value, excluding drug evidence.

(2) Seized currency subject to criminal or civil forfeiture is to be delivered to the U.S. Marshals Service for deposit in the Seized Asset Deposit Fund, and such transfer is to be recorded by the ECT in Collected Item. However, if the seized currency serves a significant independent, tangible, evidentiary purpose, i.e., presence of fingerprints, packaging in an incriminating fashion, or the existence of a traceable amount of drug residue on the bills, the currency is retained pending final disposition of the investigative matter.

(3) Valuable evidence is to be independently counted/verified by two officials. The sealing official is to be a federal criminal investigative agent or deputized officer; the witnessing official may include the ECT, the paralegal specialist, or other support employee directly involved in the processes of seizing, packaging, and initial documentation of the evidence. They are to verify the accuracy of the count and/or detect any errors before the evidence is sealed and placed in storage.

(a) The valuable evidence is placed in an appropriate-sized plastic evidence pouch. The FBI evidence label, FD-723, is to be completed with the following information:

1. Field Office Name

2. File Number

3. Date of Seizure or Purchase

4. Sealing Official's Printed Name

5. Sealing Official's Signature

6. Witnessing Official's Printed Name

7. Witnessing Official's Signature

8. Laboratory Examiner's Signature

9. Weight (for drugs)

10. DEA Exhibit Number (for drugs)

(b) The completed FBI evidence label (FD-723) is placed on the outside of the plastic evidence envelope, at the top, and folded at the perforation over both sides of the envelope. Insert the envelope into the heat sealer ensuring that the heat seal is made across the evidence label (FD-723).

(c) The Agent submitting the valuable evidence to the ECT must remain with the ECT while he/she processes the evidentiary property and until the VWO arrives to access the vault and witness the storage of the valuable evidence.

(d) Opening and resealing of valuable evidence must be conducted in the presence of:

1. Two federal criminal investigative agents/deputized officers, or

2. One federal criminal investigative agent/deputized officer and one witnessing official (as described in paragraph (3) above), or

3. Two paralegal specialists (one of which serves as a sealing official and one as a witnessing official)

(e) The reasons and procedures must be fully documented in an FD-302 by the sealing and witnessing officials. Two copies of the FD-302 are to be generated--one is designated for the investigative case file, and a second copy is to be presented to the ECT with the resealed evidence. (The ECT is to maintain the ECR copy of the FD-302 in a binder from inspection to inspection.)

(f) A plastic evidence pouch is opened by cutting off the sealed upper edge with scissors or a paper cutter, ensuring that the FD-723 is intact. If the evidence is to be resealed, both portions of the used pouch are to be retained, placed in a new evidence pouch with the evidence, and sealed following the above- mentioned instructions. Opening and resealing evidence is to be continued in this fashion.

(g) If valuable evidentiary items are of such size as to preclude the use of a plastic evidence pouch, i.e., paintings, the property should be boxed or wrapped in brown paper and secured with plastic fiber-reinforced tape ensuring that the tape encircles the package and that the tape ends meet or overlap. The FD-723 label is to be completed with all pertinent information and affixed to each box top or package front to ensure that it covers both ends of the plastic fiber-reinforced tape. The label should be covered with clear plastic tape to ensure that names are not obliterated during transport and handling.

(h) When large valuable evidentiary items are required to be opened, it is done so by first cutting the FD-723 from the front of the package or top of the box. If the evidence is to be resealed, the previously used FD-723 is placed in a plastic envelope inside the new package or box, and the new package or box is then sealed following the above-mentioned instructions.

(4) Valuable evidence must be afforded maximum security while in the FBI's possession, and not co-mingled with any other type of evidence. Storage should be in one or more of the following types of facilities:

(a) b2

(b)

Open-shelf filing is permissible in

(c)

b2

Exterior ventilation for the storage of odoriferous substances and the health and safety of evidence personnel is to be afforded. Open shelving is permissible.

(d)

Exterior ventilation for the storage of odoriferous substances and the health and safety of evidence personnel is to be afforded.

Open shelving is permissible.

(e)

(f) A separate Form FD-455 is to be maintained for each valuable repository. (See 2-4.4.12.)

(g) The ECT/AECT is not authorized to access the drug/valuable storage facility unless accompanied by the AO, or the person(s) designated to act on behalf of the AO as the VWO. The vault witness responsibility remains with the AO, but the actual duty may be delegated to meet the requirements of the field office and resident agencies. However, the VWO should not be an AECT. Each office should limit the number of designated VWOs and must document the list of authorized vault witnessing personnel in the evidence control file.

(h) The only persons having emergency access to the drug/valuable storage facility (both combinations or both keys) and the ECR is the SAC, the ASAC(s), and the Supervisory Special Resident Agent. The written access numbers to the combination(s) (or the key(s) for the dual access entry to the drug/valuable vault) must be stored separately. One combination (or key) is to be maintained in a GSA-approved security container with the central combination record file; the other combination (or key) is to be placed in the COMSEC Vault safe.

2-4.4.9 Temporary Storage - Drug and Valuable Evidence (See MAOP, Part II, 2-4.4.7 and 2-4.4.8.)

(1) A security-type safe with a dual-combination locking system may be used for TEMPORARY STORAGE of drug and valuable evidence not to exceed ten (10) calendar days from date of acquisition. The secure container should be located either outside the ECR or in the Night Supervisor's working area. The container should be secured to the floor. The contents of the night depository safe must be removed at the beginning of each work day by the ECT, accompanied by the VWO, properly stored in the ECR pursuant to established policy, and entered into Collected Item. Evidence that is being temporarily stored within the container is to be properly heat-sealed and appropriate documentation is to be attached prior to its temporary storing.

(2) Neither the SAC's safe nor a squad supervisor's safe are to be used for the temporary storage of drug/valuable evidence. In those instances when seizures of drug/valuable evidence are anticipated during off-duty hours (nights, weekends/holidays), the services of the ECT/AECT should be utilized to assist with the analyzing, cataloging and labeling of the evidence.

2-4.4.10 Storage of Evidence in Resident Agencies (RAs)

(1) Evidence that is needed at the RA for Agent review, court proceedings, etc., must be charged out by the ECT to the appropriate Agent, who is then responsible for storing it securely. Evidence that is seized, subpoenaed, or voluntarily contributed, and not relinquished to the ECT for processing into Collected Item, must be stored temporarily within RA space in a security-type safe.

(a) Access to the temporary storage facility is limited to the appropriate Agent, and the Senior Supervisory Resident Agent (SSRA) or Senior Resident Agent (SRA).

(b) An FD-455 is to be maintained for the facility and each instance of access must be recorded thereon to include the signature of the person(s) gaining entry, reason for entry, case file number and 1B number, and the date and time of entry/exit to successfully defend any chain-of-custody challenges.

(2) At the discretion of the SAC, an ECR may be established in an RA in accordance with the guidelines set forth in 2-4.4.2 and all rules and regulations applicable to evidence storage and handling applies. Drug and valuable evidence may be stored within the ECR as set forth in 2-4.4.7 and 2-4.4.8, or may be stored in a bank safe-deposit box. An employee in the RA is to be designated an ECT, and is directly responsible for the recordkeeping, storage, and maintenance of evidence in the RA. In the event bank safe-deposit boxes are used and the designated RA/ECT is a support employee, he/she must be escorted to and from the bank by the VWO.

(a) Form FD-455 (Access Log - Evidence Storage Facility) is to be maintained for the ECR and the drug and/or valuable repository, whether located within the ECR or in a bank safe-deposit box. Each instance of access must be recorded on the FD-455 to include the signature of the person(s) gaining entry, reason for entry, case file number and 1B serial/exhibit number, and the date and time of entry/exit to successfully defend any chain- of-custody challenges.

(b) Access to the RA/ECR and/or bank safe-deposit box is strictly limited to the RA/ECT and the SSRA/SRA. Access by other employees is prohibited unless accompanied by the RA/ECT and SSRA/SRA. Access is to be documented on Form FD-455. For access to the drug/valuable evidence storage facility, whether located within the field office or in a bank safe-deposit box, the RA/ECT is accompanied by the SSRA/SRA, who is the VWO. If the drug/valuable evidence is stored in a safe-deposit box, the names of the RA/ECT, SSRA/SRA are to appear on the bank access signature card, and documented in the field office evidence control file by electronic communication (EC) and updated as necessary.

(c) The RA/ECT ensures the following:

1. That the evidence is entered Collected Item within 10 calendar days.

2. If the evidence is submitted late, an EC must accompany the evidence before being entered into Collected Item.

3. That a 1B serial number is recorded on the automated FD-192 for file.

4. That the evidence is bar coded.

5. That an automated FD-192 is initialed by the SSRA/SRA and filed in the case file; a second copy is attached to the property; and a third copy is made for forfeiture.

6. That chain-of-custody documentation is recorded in Collected Item and on the automated FD-192 maintained with the evidence.

7. That an FD-302 is completed when evidence is to be resealed.

8. That evidence is properly packaged when the need arises to mail.

9. That disposition information is recorded in Collected Item.

10. Retrieves evidence from RA/ECR when need arises and ensures chain of custody is accurately recorded in Collected Item and on the automated FD-192.

11. Produces every 60 days a charge-out reminder report for evidence charged out from RA/ECR.

12. Disposes of property on instructions of SA personnel by appropriate methods.

13. As necessary, may be required to testify in a court of law regarding evidentiary property for which responsible.

(For detailed responsibilities of the ECT, see 2-4.4.3.)

2-4.4.11 Transmittal of Evidence to Field Offices and FBIHQ/DEA Laboratories (See MAOP, Part 2, 2-2.2.2(1)(i).)

(1) The ECT is responsible for properly preparing evidence for mailing/shipping. Refer to MIOG, Part 2, Section 13, and the HANDBOOK OF FORENSIC SCIENCE for illustrated packaging chart and related information.

(a) For shipping of drug and valuable evidence, the case Agent is to ensure that the evidence is properly heat-sealed prior to being packaged for shipment. Due to the fact that drug/valuable evidence is not to be left solely in the custody of the ECT, the case Agent/acquiring Agent and/or the VWO is to witness the wrapping/packaging of such evidence by the ECT for shipment.

(2) Due to chain-of-custody requirements, ALL EVIDENCE TRANSMITTED BETWEEN FBI OFFICES IN THE U.S. AND PUERTO RICO, IS TO BE SENT BY EITHER U.S. POSTAL SERVICE USING ONLY REGISTERED MAIL, OR BY FEDERAL EXPRESS. However, Classified National Security Information shall be transmitted according to its classification level as prescribed in MIOG, Part 2, 26-7. (When U.S. Registered Mail is used, Form FD-441a (Return Receipt for Evidence Control Technician) must be completed, and placed in the outer evidence packaging. If Federal Express is utilized, never use their "drop-off" service. Ensure that the package is picked up and a receipt is received.) Regardless of the mode of shipping, clear yellow evidence tape must always be placed over the shipping address label.

(a) Evidence that is shipped to other agencies is to be shipped via U.S. Registered Mail, return receipt requested (PS 3811.) The receipt is then placed in the 1A section of the investigative case file. (See 2-4.4.13.)

(b) Evidence that is being returned to the contributor/owner is to be shipped U.S. Registered Mail, return receipt requested (PS 3811.) (See 2-4.4.17.) The receipt is then placed in the 1A section of the investigative case file.

(3) If evidence is being transmitted from one field office to another, the evidence must first be entered and disposed in Collected Item.

(a) The ECT in the transmitting office prints out two copies of the automated FD-192. The file copy is initialed by the Squad Supervisor, and filed in the investigative case file. (If the case file is in the office of origin (OO) and it is the lead office (LO) that is shipping the evidence to the OO, then the file copy of the FD-192 and all other appropriate documents required by the investigative case file are to be shipped to the OO with the evidence.) (Drug and valuable evidence must be appropriately sealed before being transmitted.) The package copy of the automated FD-192 must accompany the evidence that is being shipped. When transmitting to the FBI or DEA Laboratories, the package copy of the automated FD-192 remains filed in a binder marked "(Name of Office) - Evidence sent to FBI Lab" or "(Name of Office) - Evidence sent to DEA Lab." The binder is maintained in the ECR. (See Section 2-4.4.4.)

(b) The ECT in the transmitting office will record the manual chain of custody on the automated FD-192 maintained with the evidence:

Received By: Honolulu Remarks: Sent via FEDEX 123456789 (or Reg 246) w/EC dated 2/23/96

The ECT in the transmitting office will also record the automated chain of custody in Collected Item:

Accepted Date.>> 02231996 Accepted Time.>> 0200pm Accepted By....> Organization..>> Honolulu Reason.....>> Forwarded Remarks.....> Sent via FEDEX 123456789 (or REG 246) w/EC dated 2/23/96

(c) The FD-441a is for FBI use only. This form is to be executed by the ECT in the transmitting office and placed in the package with the evidence when the evidence is being shipped via U.S. Registered Mail.

(d) The ECT in the receiving office must complete the remaining portion of the FD-441a (if U.S. Registered Mail was utilized) and return it to the sending office, Attention: ECT. The receipt is then placed in the 1A section of the investigative case file.

(e) In the receiving office, the cover sheet of the package copy of the automated FD-192 that accompanied the evidence is filed in a 1A envelope in the appropriate case file. The ECT then enters the evidence into Collected Item, giving it a 1B number for his/her office. He/She then generates three new automated FD-192s (for the file, for the evidence, and for forfeiture) to document the receipt of the evidence in the receiving office. The original chain of custody (that accompanied the evidence) is attached to the newly computer-generated FD-192, is appropriately signed, and remains with the evidence in the receiving office.

Page One of the "Received Collected Item" (formally known as the Group Information) will read as follows:

Category.....>> 1B Acquired Date...>> 02261996 Acquired Time...>> 1000am Acquired By.....>> (name of ECT in receiving field office) Contributor.....>> (name of transmitting field office)

(4) If evidence is being transmitted from a field office to FBIHQ or DEA Laboratory, it must first be charged out manually and documented in Collected Item. Drug and/or valuable evidence must be sealed prior to being shipped.

(a) The ECT in the transmitting office will record the manual chain of custody on the automated FD-192 maintained with the evidence:

Received By: FBI Lab (or DEA Lab) Remarks: Sent via FEDEX 123456789 (or REG 246) w/EC dated 2/23/96

The ECT in the transmitting office will also record the automated chain of custody in Collected Item:

Accepted Date.>> 02231996 Accepted Time.>> 0200pm Accepted By....> Organization...> HQ (or DEA) Reason.....>> Analysis Remarks.....> Sent to FBI Lab (or DEA Lab) via FEDEX 123456789 (or REG 246) w/EC dated 2/23/96

The package copy of the automated FD-192 is retained in the ECR and filed in a binder/folder labeled "Evidence Sent To FBI (or DEA) Laboratory" according to date of transmittal.

(b) The FD-441a is to be completed by the ECT in the transmitting office (if U.S. Registered Mail is utilized), and placed inside the outer packaging with the evidence that is to be transmitted between field offices, and field offices and FBIHQ. DO NOT use Form FD-441a when transmitting evidence to DEA.

(c) The FBIHQ Laboratory and field offices must complete the remaining portion of the FD-441a (if U.S. Registered Mail is utilized) and return it to the sending office, Attention: ECT. The receipt is then placed in the 1A section of the investigative case file.

(d) When the evidence is returned, the ECT is to record chain of custody on the automated FD-192 maintained with the evidence and in Collected Item. If general evidence, affix the package copy of the automated FD-192 to the evidence. If drug or valuable evidence, place the package copy of the automated FD-192 in the binder maintained in the drug/valuable vault.

(5) As a general rule, evidence seized/recovered by RA personnel is stored in Headquarters City and transmittal of such evidence to another field office/FBIHQ/DEA Laboratory is handled by the Headquarters City ECT. However, if an ECR has been established in a RA, evidence must be administratively handled and entered into Collected Item prior to being wrapped/packaged/shipped by the RA/ECT according to the aforementioned guidelines. Otherwise, RAs may only transmit evidence directly to another field office/FBIHQ/DEA Laboratory in instances where the urgency of a particular situation demands expedient handling, or in instances when the bulk of the evidence is such that to ship through Headquarters City for subsequent shipping elsewhere would be impractical. In such instances where FBIHQ/DEA Laboratory returns evidence directly to an RA, a copy of the communication transmitting/returning the evidence must be furnished to the Headquarters City ECT for appropriate administrative handling, when the RA does not have an established ECR.

(6) Before filing or forwarding obscene and indecent matter which has come into the possession of an employee during the course of an investigation, it shall be placed in a sealed container and the container marked for identification and the label marked "Obscene." Such evidence is considered general evidence and stored in the ECR. (See MAOP, Part 2, 2-4.4.4 (20) ; MIOG, Part 1, 145-2; Correspondence Guide-Field, 1-14.)

(7) For the handling, transportation, shipping, and storage of explosives, see MIOG, Part 2, 13-16.2 and 13-16.3, and the HANDBOOK OF FORENSIC SCIENCE.

2-4.4.12 Charge-Out Procedures - Evidentiary Property (See MAOP, Part II, 2-4.4.8 and 2-4.4.16.)

(1) Evidence stored in the ECR, or other evidence storage facilities, may be charged out to any employee having an official need. Evidence may be charged out for up to 60 calendar days and recharged at the end of those 60 days and, if necessary, every 60 days thereafter as follows:

(a) The ECT is to record chain of custody on the automated FD-192 and in Collected Item.

(b) The package copy of the automated FD-192 must remain with the evidence. Care should be exercised by the employee accepting custody of the evidence to ensure that chain-of-custody information is recorded on the package copy of the automated FD-192.

(2) The ECT must run Collected Item charge-out reminders, and recharge evidence every week or every two weeks, depending on the size of the field office.

(3) If the evidence is to be recharged, the person to whom the evidence is currently charged must initial next to that item on the Evidence Charge-Out Report and return the report to the ECT. If the evidence is no longer required to be charged out, the person to whom the evidence is currently charged immediately returns the evidence to the ECR for storage.

(4) Two copies of the Charge-Out Report should be printed by the ECT. One copy is forwarded to the appropriate squad supervisor for initialing by appropriate squad personnel. The second copy is maintained by the ECT, to reconcile responses from each Squad/RA. Charged-out evidence will appear on the Charge-Out Report at 60-day intervals until the evidence is returned to the ECR for storage.

(5) Upon return of the evidence, the ECT records chain of custody on the automated FD-192 and in Collected Item. Once all charged-out evidence has been accounted for, both copies of the Charge-Out Report are to be discarded.

(6) When evidence is accessed by Agent personnel for review/examination outside the ECR, or in the "reception area" of the ECR, chain of custody must be executed on the automated FD-192 maintained with the evidence and in Collected Item. If the review/examination takes place in the "reception area" of the ECR, the FD-455 need not be completed, as the visitor did not enter the actual ECR where the evidence is stored.

2-4.4.13 Evidence Released to Custody of Outside Agencies (See MAOP, Part II, 2-4.4.11.)

(1) When evidence is permanently released to the custody of an outside agency, disposition and chain-of-custody documentation is to be recorded on the package copy of the automated FD-192 and in Collected Item. A receipt for the property (Form FD-597) must be signed by the person representing the receiving agency and then filed in the 1A section of the investigative case file. When money is involved, the receipt should clearly indicate that the receiving agency counted the money and that the amount corresponds to the amount listed on the original documentation.

The ECT is to:

(a) Place the package copy of the automated FD-192 in the 1A section of the investigative case file. The chain of custody will show the signature of the Agent who charged out the evidence, followed by a statement showing release of the evidence to the receiving agency. For example:

Received By: [redacted] 1/8/96 2pm Remarks: Review Received By: Released to USM [redacted] 1/8/96 3pm Remarks: See FD-597 dated 1/8/96

b6
b7C

(b) Make an appropriate notation on the file copy of the FD-192 (which is in the investigative case file) regarding the disposition, i.e., "Released to the custody of USM [redacted] by SA [redacted] on 1/8/96 - See 1A-5."

(c) Modify Collected Item to reflect the chains of custody and disposition.

Chain = Accepted Date..>> 010896 Accepted Time..>> 0200pm Accepted By.....> [redacted] Organization....> Reason.....>> Review Remarks.....> Probable release to USM

Disposition = Disposal Method>> USMO Disposal Date..>> 01081996

Chain = Accepted Date..>> 010896 Accepted Time..>> 0300pm Accepted By.....> Organization....> USMO

Reason.....>> Released Remarks.....>> Released to custody of USM [redacted] see FD-597 1/8/96

If one or several items, as opposed to all items listed on the FD-192 are released, perform the "Split" function in Collected Item, and make appropriate notations on the file copy of the FD-192 and on the new chain of custody. A new package copy of the automated FD-192 is printed and is attached to the original chain-of-custody page for the remaining item(s), and is maintained with the remaining item(s) of property pending final disposition of all items. (See the ACS USER'S GUIDE for detailed instructions on the splitting of evidentiary items.)

(2) When property is temporarily released to an AUSA or non-Task Force officer, the Agent charging out the evidence signs the chain of custody and retains the package copy of the FD-192 (with chain of custody attached) until the evidence is returned to him/her. The non-Task Force officer signs a receipt (FD-597) for the property. The receipt is attached to the FD-192 until the evidence is returned to storage, at which time the receipt is then placed in the 1A section of the investigative case file. (AUSAs do not sign chains of custody nor FD-597s.)

2-4.4.14 Handling of Evidence and Property by the U.S. Marshal (Moved from 2-4.4.2.)

(1) Where it can be arranged to the satisfaction of the U.S. Marshal (USM) and the SAC, property seized as evidence should be turned over to the USM. However, no attempt should be made to store with the USM items not known to be evidence. U.S. Marshal's Manual, Section 541, dated December 15, 1971, provides that "Marshals are authorized and instructed to accept, store, and safeguard all items to be used in evidence, and all nonevidentiary property involved in violations of federal gambling laws, which have been seized by the F.B.I. incident to an arrest or in connection with searches and seizures under warrants. Only such property as is to be used in evidence or seized for gambling violations should be accepted. The storage of any other property in the possession of the F.B.I. is the responsibility of the Bureau representatives. Any questions as to whether particular property will or may be used in evidence will be resolved by the U.S. Attorney of the District where the property is to be stored." The SAC is responsible for ensuring proper storage and security of such property. If deemed necessary, FBIHQ assistance should be solicited. The USM will give a receipt for property stored under USM's custody, keeping a copy of the receipt accurately describing the property received. The USM's Manual further instructs that "seized money will be counted in the presence of the person from whom it is received, and both the Marshal and the person delivering the money will sign the receipt." The USM will return seized property or evidence to the owner or other person designated, or otherwise dispose of it in accordance with a court order or written instructions from the USA. Receipts obtained for property released to the custody of the USM should state that the property has been verified by the USM, and when money is involved, the receipt should clearly indicate the USM has counted the money and the amount is correct. These receipts should be filed in the 1A section of the investigative case file. (See MIOG, Part 1, 91-13.8.)

(2) When property is seized as evidence and it is of such a nature that its bulk (i.e., an automobile) and other circumstances would bring it within the purview of USM's Manual, Section 541, ensure by contacting the USA that USA desires the matter to be held as evidence for future court action. A letter to this effect should be obtained from the USA, or if an oral opinion is given, it should be confirmed in writing by the field office. A copy of the correspondence should be furnished to the USM and it should be made clear to all parties concerned in writing that the USM is holding the item or items as evidence.

(3) The foregoing procedure does not alter in any manner the prevailing FBI instruction that Agents should not take possession of a stolen motor vehicle (ITSMV case). If a special problem arises in an ITSMV case in which the automobile may also be an item of evidence, the situation should be discussed with the USA and handled in accordance with the above-outlined procedures. To assist in gathering complete data regarding the recovered vehicle, the FD-653, Motor Vehicle Inspection Inventory Record, may be used. The FD-653 is an optional administrative form which, if used, is to be retained in the 1A section of the investigative case file, with the Agent's notes.

(4) A consolidated record is to be maintained of all property released to the custody of the USM. This may be accomplished by placing in a folder entitled "Record of Evidentiary Material in Possession of USM" a reproduced copy of the FD-192 and/or the 1A evidence envelope, FD-340, FD-340b and/or FD-340c, bearing appropriate notation of disposition of the evidence or portion of

the evidence. Otherwise, a log of such items may be maintained, identifying the items by file number, subject of case, description of item(s), and date released to the USM. These records are to be reconciled annually with corresponding records of the USM to ensure their accuracy. Any differences or inaccuracies are to be immediately resolved. This is to be accomplished at the time of the inventory of the general evidence, and a notation certifying to the accuracy of the records affixed to the FBI copy of such record along with the date and name of the employee who made the comparison.

2-4.4.15 Physical Audit/Inventory - Evidentiary Property (See MAOP, Part 2, 2-4.4.4.)

(1) AN AUDIT (physical/telephonic/written verification of evidence charged out) coupled with AN INVENTORY (automated scanning of bar codes attached to evidence (or primary evidence container) housed in an ECC), is to be conducted as follows:

(a) A 100 percent unannounced audit/inventory of general evidence (to include firearms, federal grand jury and CART) and charged out evidence, at least once in a calendar year as determined by the SAC/AO (not to be conducted at the same time each year).

(b) A 100 percent unannounced audit/inventory of drug and valuable evidence and charged out evidence at least once in a calendar year as determined by the SAC/AO (not to coincide with the inventory of general evidence nor to be conducted at the same time each year).

(c) A 100 percent audit/inventory of general (to include firearms, federal grand jury and CART), drug, and valuable evidence and charged out evidence, PRIOR TO THE DEPARTURE of the AO.

(d) A 100 percent audit/inventory of general (to include firearms, federal grand jury and CART), drug, and valuable evidence and charged out evidence, PRIOR TO THE DEPARTURE of an ECT/AECT position(s) in HQ city (or in an RA that has an ECT/AECT departing).

(e) A 100 percent audit/inventory of all evidence before and after the relocation of a field office, RA, and/or ECR (within 30 days of the move).

(f) At any time an SAC/AO deems an inventory to be necessary.

(2) The SAC/AO is to designate an Agent(s) and/or support supervisor who does NOT have a direct supervisory role in the Evidence Program and/or an FBI Auditor to conduct the inventory/audit and to write the accompanying electronic communication (EC).

(3) The SAC/AO is to designate an RA Agent and/or RA support supervisor who does NOT have a direct supervisory role in the Evidence Program to conduct the audit/inventory of approved ECRs/ECCs in resident agencies and the writing of the accompanying EC.

(4) THE ECT/AECT IS NOT TO CONDUCT AN AUDIT/INVENTORY, NOR WRITE THE ACCOMPANYING EC. However, the ECT/AECT must be present in the designated ECR throughout the entire audit/inventory process to ensure the integrity of the evidence, and resolve any discrepancies that may develop.

(5) During an audit/inventory of the Drug and Valuable ECRs, the Vault Witnessing Official (VWO) MUST remain inside the designated ECRs throughout the entire audit/inventory process.

NOTE: VWO's have a role in the Evidence Program by their witnessing duties and, therefore, are exempt from conducting audit/inventories.

(6) The Agent/support supervisor/auditor who is designated to conduct an audit/inventory must sign in/out on the FD-455 maintained for each ECR that they access in order to conduct the audit/inventory. The chain-of-custody is NOT TO BE SIGNED by the employee(s) conducting the audit/inventory unless they take physical custody of the evidence.

(7) Sealed drug and valuable evidence KPAKs/boxes are NOT TO BE OPENED for an audit/inventory nor inspected. If a seal is found to be improperly sealed/broken or has dried and therefore has opened, the person conducting the audit/inventory is to immediately notify the case Agent/sealing Agent so that the evidence may be immediately resealed/repackaged and updated in the evidence database.

(8) An INVENTORY is to entail the automated scanning of all bar codes that are affixed to evidence (or the primary container) housed in the ECR that is being checked. Once scanned, the bar codes are uploaded, and an Exception Report is produced. An AUDIT is to be a physical, telephonic and/or written verification by the person conducting the audit/inventory to ensure that the evidence, said to be charged to a specific employee, is, in fact, in the custody of that employee.

(9) An EC to the SAC/AO, documenting that an audit/inventory of evidentiary property (name the type of evidence, general (to include firearms, FGJ and CART), drugs, valuables) was conducted is to be PREPARED BY THE AGENT/SUPPORT SUPERVISOR/AUDITOR WHO CONDUCTED THE AUDIT/INVENTORY. The approved/uploaded/serialized EC is then placed in the field office Evidence Control Subfile designated for the audit/inventory of evidence. The EC should reveal the date(s), name(s) of individual(s) who conducted the audit/inventory, any deficiencies detected, and steps taken to resolve those deficiencies. The EC is to be maintained from field office inspection to inspection. The final copy of the Exception Report is to be included as an enclosure to the EC. Separate ECs are to be done for each type of audit/inventory conducted.

(10) The EC should contain a lead for the Laboratory Division, Attention: Evidence Program Manager, for information purposes. (Copies of the Exception Report are NOT to be sent.) If there are any unresolvable errors, the EC is to so state, as well as the steps being taken to resolve the problem. If the SAC recommends administrative action, this is to be so noted in the documentation to the FBI Evidence Program Manager.

2-4.4.16 Nonevidentiary Property (Revised and Moved from 2-4.4.4.) (See MIOG, Part 2, 2-9.5.)

(1) 1A Serials:

(a) 1A serials are documents or items of property which are pertinent to an investigation. Generally the size, nomenclature, and/or value of the nonevidentiary item will determine the place where it is to be filed; however, all physical evidence seized or contributed incidental to a search by search warrant, arrest, or crime-scene search, that requires a chain of custody, must be maintained in the Evidence Control Room (ECR) as 1B evidentiary property.

(b) If the evidence is not likely to come under attack regarding chain of custody, and is of such size that it can be filed in the investigative case file, it is to be placed in a white evidence envelope

(Form FD-340, FD-340b and/or FD-340c) showing the universal case file number and serial number of the item, the date received (by investigating employee), name and address of contributor, whether it may be returned, whether a receipt was given, and description of the evidence. The serial number of the document in the investigative case file that originated and identifies the 1A may be recorded on the FD-340, FD-340b and/or FD-340c at the discretion of the case Agent. The FD-340, FD-340b and/or 340c is to be placed inside the 1A envelope, FD-340a, which is a letter-sized envelope known as the 1A serial in the investigative file. Due to the size of the FD-340c, it can be placed in front of the FD-340a inside an accordion-type folder. The FD-340a envelope is placed at the bottom of the file under serial number one. The FD-340a shall be clearly marked as to contents and shall bear the date the FD-340, FD-340b and/or FD-340c was placed in the FD-340a, and file, and serial number. If the number of FD-340's, FD-340b's and/or FD-340c's in the FD-340a envelope increases to the point where the file is unwieldy, a subfile must be opened and filed adjacent to the investigative case file.

(c) In zero and control files, the FD-340a evidence envelope is to be filed adjacent to the EC, letter, or other communication to which it pertains.

(d) When transmitting 1A evidence to another field office, leave the evidence in the white evidence envelope (FD-340, FD-340b and/or FD-340c) and place a notation on the FD-340a 1A evidence envelope to show disposition and describe the method of transmittal. Transfer Collected Item to show the field office the 1A was sent to and the date it was transferred. Do not send FD-340's, FD-340b's and/or FD-340c's to FBIHQ. If a portion of the evidence is being transmitted, prepare an FD-340, FD-340b and/or FD-340c for the receiving office in the same fashion as above and place appropriate notations on the FD-340a. No outer enclosure envelope is required.

(2) Bulky Nonevidentiary Material:

(a) If other nonevidentiary bulk property which may be pertinent to an investigation and must be retained is of such size that it cannot be filed in the 1A section (FD-340a) of the investigative case file, it is to be made a 1C, documented on Form FD-192a, and recorded in the investigative case file. The material is to be stored segregated from evidentiary property and access restricted to those persons with an official need. (See 2-4.4.4.)

(b) The drafted FD-192a and the property is to be furnished to the ECT. (Form FD-340/FD-340b/FD-340c is to be furnished to the Information Management Assistant/Clerk (IMA/IMC) working the specific squad rotor.)

(c) Collected Item will computer-generate the 1A/1C serial number. The ECT/IMA will enter the exact storage location.

(d) One copy of the automated FD-192a is to be filed in the 1C section of the investigative case file. (The FD-340/FD-340b/FD-340c is filed in the 1A section (FD-340a) of the investigative case file.)

(e) A second copy of the automated FD-192a is to be affixed to and remains with the property until final disposition.

(f) When nonevidentiary property is required to be charged out, it is done so by using Form FD-5 (Serial Charge-Out). Personnel having an official need may charge out nonevidentiary property for

up to 60 calendar days, and if necessary, recharge every 60 days thereafter. (See MIOG, Part 1, 91-13.8.)

(3) Nonevidentiary property entered into Collected Item is handled in the same manner as evidentiary property. However, a chain of custody is not required, and an inventory is not conducted.

(4) Federal Grand Jury (FGJ) Material:

(a) Access to FGJ material must be limited to authorized persons appearing on the FGJ list, and when not in use must be placed in a secured location. The FGJ list may be the Rule 6(e) letter of the Assistant United States Attorney (AUSA), or (with the concurrence of the USA's office) an FBI internal certification list. (See MIOG, Part 2, 2-9.6.1.)

(b) Absent chain-of-custody requirements, the material is to be placed in a subfile which is locked in a container (or room) with a combination lock, the combination of which is known only by such authorized persons appearing on the FGJ list. The combination(s) is to be changed annually. The material is documented on Form FD-192a in a timely fashion. When the material is required to be charged out, Form FD-5 is utilized. Please note that when a secured room is used, rather than separate secured containers, individuals with access to that room must be listed on the FGJ lists of all cases that are in that room. (See MIOG, Part 2, 2-9.7 (2).)

(c) When a chain-of-custody is required, the material is treated in accordance with the rules and regulations pertaining to general evidentiary property, i.e., documented in the investigative case file within 10 calendar days on Form FD-192. (See 2-4.4.12.) However, the material is stored segregated from all other types of general evidence in either a separate room with a combination lock (used exclusively for the storage of evidentiary FGJ material), or a separate container within the ECR, or on separate shelving within the ECR. When a separate room is utilized, a separate Form FD-455 (Access Log-Evidence Storage Facility) is to be maintained. The ECT, and in his/her absence, the Alternate ECT, accesses the material, as is the rule with all evidentiary property. When the need arises, appropriate charge-out procedures are utilized. (See MAOP, Part 2, 2-4.)

(d) Evidentiary and nonevidentiary FGJ material must never be co-mingled for storage purposes.

2-4.4.17 Disposition of Property

(1) When an investigative case is closed, it is the responsibility of the case Agent to dispose of seized/recovered/ contributed property when there is no further need for retention. Whenever there is any doubt regarding the need for retention, the AUSA should be consulted and the contact recorded in the investigative case file.

(2) Certain case files will be marked for "Permanent Retention" and will eventually be transferred to the National Archives and Records Administration. In such instances, only those evidentiary and nonevidentiary exhibits, regardless of size, that are documentary in nature, generated by and considered FBI records (i.e., Agents' interview notes, photographs, work papers, ledgers, journals, etc.), are to be preserved as part of the case file. Documentary materials (i.e., records of private enterprises, original or copies, contributed, seized or subpoenaed) should be returned to the rightful owner when the investigative or administrative purpose for which they were obtained has been satisfied. (See also MIOG, Part 2, Section 28, and Legal Handbook for Special Agents, 5-13.4.)

Likewise, physical property (i.e., typewriters, radios, televisions, firearms, etc.) is to be returned to their rightful owner.

(3) Guidelines for the disposition of drug evidence are contained in the Manual of Investigative Operations and Guidelines (MIOG), Part I, Section 281-8.

(4) Guidelines for the disposition of firearms are contained in the MAOP, Part 2, 2-4.4.6.

(5) Detailed procedures for disposition of forfeited and abandoned property are contained in the Forfeiture Manual.

(6) The following procedures should be followed for disposing/returning of general and valuable evidence in a closed investigative case:

(a) The case Agent and/or ECT (when advised in writing via an EC by the case Agent) should make every effort to notify the owner/contributor of the property, telephonically or in writing, advising that their property may be reclaimed within 30 calendar days and will be released to him/her or his/her authorized Agent. Record in the case file the fact that the contact was made.

(b) If property is personally returned to the owner/contributor, Form FD-597 is to be properly executed. The original of the FD-597 is to be placed in the 1A section of the investigative case file.

(c) If the owner/contributor requests that the property be returned by mail, it is to be sent by U.S. Registered Mail, return receipt requested. When the return receipt (Postal Form 3811) is returned to the field office, it is to be placed in the 1A section of the investigative case file. Form FD-631 (Return of Seized/Recovered Property), a preprinted transmittal letter, is to accompany the property when the property is returned to the owner by mail. The FD-631 should request that the owner sign the enclosed FD-597 and return it in the attached postage-paid, self-addressed envelope. The FD-597 should detail the exact property being returned. When the FD-597 is received by the field office and signed by the owner of the property, the original is to be placed in the 1A section of the investigative case file. (See MAOP, Part 2, 2-4.4.11.)

(7) The ECT is responsible for ensuring the following recordkeeping procedures are followed when evidentiary and nonevidentiary property is disposed of:

(a) The package copy of Form FD-192 should have a completed chain of custody reflecting the disposition. Form FD-192a should also reflect the disposition by the placing of a notation. Forms FD-192/FD-192a are then placed in the 1A section of the investigative case file. Collected Item must be modified to reflect the date and method of disposition. Ensure that the disposition is reflected in the disposition field and on the automated chain of custody.

(b) If one or several items, as opposed to all items listed on Forms FD-192/FD-192a are disposed of, the package copy of the FD-192/FD-192a is to be kept with the remaining items of property pending final disposition of all items.

(8) A notation is to be placed on the closing communication indicating that property acquired during the investigation has been disposed of, disposal is being initiated, or stating a valid reason for retention. Supervisors may not approve the closing of cases in which property has been seized/recovered/contributed without the appropriate notation.

(9) Retention of evidence/nonevidence in closed cases can be monitored through the ACS to:

(a) Provide supervisory personnel the tools to enforce prompt property disposition through the case review process;

(b) Provide field office management statistical reports to identify individuals/squads which are not in compliance with property disposition procedures; and

(c) Highlight noncompliance trends to the Inspection Staff for evaluation.

The report "Closed Cases With Pending Collected Item," is to be printed and distributed to appropriate case Agents at 60-day intervals by the ECT to ensure that those items eligible for disposition are handled. If evidence is to be retained for an extended period of time, the case Agent should so indicate by recording an anticipated disposition date and his/her initials on the report. (An EC to the investigative case file is then required explaining the reason for retaining the evidence. A copy of the EC is maintained in the ECR until final disposition of the evidence.) The report is then initialed by the supervisor and returned to the ECT. The returned reports showing retention, are to be maintained in a binder in the ECR from inspection to inspection.

2-4.4.18 Forms Used in the Evidence Program

DEA-7 Report of Drug Property Collected, Purchased or Seized

FD-5 Serial Charge-Out

FD-192 Control of General/Drug/Valuable Evidence

FD-192A Inventory of Nonevidentiary Property

FD-302 Form for Reporting Information That May Become Testimony

FD-340 1A Envelope (6 x 10 inches)

FD-340A 1A Envelope (9 x 11 1/2 inches)

FD-340B 1A Envelope (4 1/4 x 10 1/4 inches)

FD-340C 1A Envelope (8 1/2 x 11 inches)

FD-441A Return Receipt for Evidence Control Technician

FD-455 Access Log-Evidence Storage Facility

FD-597 Receipt for Property Received, Returned, Released, Seized

FD-631 Letter to Accompany Return of Documentary Evidence

FD-632 Evidence Transmittal Envelope

FD-723 Evidence Label

FD-737 Indemnity Agreement

PS-3811 Domestic Return Receipt

2-4.5 Destruction of Field Files and Records

The destruction of FBI files and records is governed by Title 44, U.S. Code, Sections 3303 and 3303a; Title 36, Code of Federal Regulations, Part 1220; the General Records Schedule (GRS); and the FBI Records Retention Plan and Disposition Schedule (The Plan) developed by the National Archives and Records Administration (NARA) and the FBI, which was approved by the United States District Court, District of Columbia, Washington, D.C., September 9, 1986.

FILES AND RECORDS NOT IDENTIFIED HEREINAFTER ARE NOT TO BE DESTROYED WITHOUT SPECIFIC FBIHQ AUTHORITY.

The following field files and records are authorized for destruction after observance of the instructions and restrictions set forth below. The file number and date of destruction are to be recorded on Form FD-478 (List of Files Destroyed/Transferred to FBIHQ). Form FD-478, containing the file numbers and dates files were destroyed, is to be maintained at the beginning of each respective classification in the closed files section. For files bearing the Universal Case File Number (UCFN), the FD-478 should be filed at the beginning of the field office breakdown in the closed files section. At the option of each office, an additional copy of Form FD-478 may be maintained in an administrative control file entitled "List of Files Destroyed."

2-4.5.1 Restrictions:

(1) Periodically, and pursuant to criteria outlined in The Plan, FBIHQ issues to the field instructions to stamp certain field files/records, including lead office files with 50 or more volumes/sections, with legends "DO NOT DESTROY: HISTORICAL VALUE - NATIONAL ARCHIVES" and/or "X: DO NOT DESTROY: HISTORICAL VALUE - NATIONAL ARCHIVES." Files so stamped are permanent and must be retained for eventual transfer to the NARA. Pursuant to the provisions of The Plan no field office may engage in file destruction of office of origin case files unless specifically authorized on case file classification basis. All time periods and cut-off dates for records destruction, as set by FBIHQ, must be strictly adhered to without exception.

(2) Freedom of Information/Privacy Acts (FOI/PA) Request:

Upon receipt of an FOI/PA request in the field office, the request must be immediately searched through the office indices to identify any relevant files which must be immediately marked to indicate that an FOI/PA request is pending and to preclude premature destruction pending resolution of the request.

(3) Litigation Matters:

No field office may engage in file destruction until all litigation matters have been searched through the office indices and relevant files identified and marked for retention pending resolution of the litigation. Case files which bear the notation that files are being retained due to pending litigation are to be maintained until notification is received from FBIHQ that the litigation has been resolved. Upon receipt of new litigation matters from FBIHQ, all file destruction must cease until the new litigation freeze sheets have been searched through the office indices and related files identified and marked for retention pending and to preclude premature destruction pending resolution of the litigation.

(4) Tax Returns/Tax Return Information:

Tax returns and/or tax return information are to be removed from lead office files prior to destruction and forwarded to the office of origin for retention in the office of origin file for five (5) years from date of receipt of the Internal Revenue Service (IRS) material from IRS, or five (5) years from the date of any disclosure, whichever is longer.

(5) Original Documents:

Original FD-302s, Laboratory reports, Latent Fingerprint reports, original surveillance logs, Agents' investigative notes, original photographs and other original documents maintained in the 1-A section of lead office case files are to be forwarded to the office of origin prior to destruction of the lead file. Form FD-491 (Transmittal of Original Documents to Office of Origin) may be used for this purpose.

(6) Office of Origin (OO) Changes:

In those cases where OO is changed, both the new OO and new lead office will apply the 10-year (criminal) or 20-year (security/applicant) destruction rule. It will be the responsibility of the new OO to advise the original OO when case is closed. This will ensure that original documents and/or evidence is not prematurely destroyed.

(7) Investigative/Administrative Needs:

Case files which continue to serve investigative, administrative or research needs may be retained if deemed necessary. If a case file that has not been marked for archival retention is retained beyond the authorized destruction period, a communication should be placed in each case file justifying the need for longer retention.

(8) Disposition of Property

(a) Certain case files will be marked with the notation "DO NOT DESTROY: HISTORICAL VALUE - NATIONAL ARCHIVES" and will eventually be transferred to the National Archives and Records Administration. In such instances, only those evidentiary and non- evidentiary exhibits, regardless of size, that are documentary in nature, generated by and considered FBI records, i.e., Agents' interview notes, photographs, work papers, ledgers, journals, etc., are to be preserved as part of the case file. Documentary materials, i.e., records of private enterprises, original or copies, contributed, seized or subpoenaed should be returned to the rightful owner when the investigative or administrative purpose for which they were obtained has been satisfied. Likewise, physical property, i.e., typewriters, radios, televisions, firearms, etc., are to be returned to their rightful owner or, if required, disposed of in accordance with approved procedures, i.e., drug evidence, illegal firearms, forfeited and abandoned property, etc.

(b) Prior to closing a case, it is the responsibility of the case Agent to dispose of seized/recovered/contributed property when there is no further need for retention. Wherever there is reasonable doubt regarding the need for retention, the United States Attorney/Assistant United States Attorney should be consulted and the contact recorded in the case file.

(c) Disposition of Drug Evidence:

See Manual of Investigative Operations and Guidelines (MIOG), Part 1, Section 281-8.

(d) Disposition of Other Property:

See Forfeiture Manual concerning property subject to forfeiture and Forfeiture and Abandoned Property Manual, Section 10, concerning abandoned property.

2-4.5.2 Destruction - Investigative Files and Records: (See MIOG, Part 1, 67-4.2.11 and 67-7.15.)

(1) Index Records/Cards: Automated index records in the Automated Case Support (ACS) data base will be deleted when the corresponding file is destroyed in the Investigative Case Management (ICM) application. Manual index records corresponding to files destroyed should be purged from the general indices at the discretion of the SAC.

(2) Copy Destruction

(a) Duplicate copies of communications, maintained within the same case file, which DO NOT contain action notations, i.e., notations issuing instructions, notations requesting action be taken, notations of certification that action was taken, etc., may be removed from those case files that have been stamped as having historical/research value (exceptional and/or permanent) when the case file is closed and destroyed.

(b) Copies of documents which contain action notations not appearing on the original file copy are to be retained within the same case file along with the original file copy.

(c) Duplicate copies of documents, maintained within the same case file, which have not been stamped as having historical/research value also may be purged and destroyed when the case file is closed. (See MAOP, Part 2, 2-4.3.1 (3)(h) & 2-4.5.3.)

(3) Record Checks:

(a) LEAD OFFICES may destroy, when six (6) months old, results of contacts with various credit, law enforcement, and federal, state and local Bureaus to determine criminal, credit and/or employment status of individuals related to current investigations.

(b) Record Checks in OFFICE OF ORIGIN are to be retained/destroyed commensurate with the disposition authority of the office of origin case file to which the record check relates.

(c) Field office files containing record checks conducted in connection with applications for employment, and resulting in receipt of information identifiable with applicant may be destroyed when six months old or when all administrative needs have been met, whichever is later.

(4) Deleted

(5) Deleted

(6) Zero "0" Files: Zero "0" files in classifications one (1) through two hundred seventy-nine (279), exclusive of classifications 192, 214, 258, 261, 267, 268, 269, 270, 271, 272, 273, 274, 275, 276, 277, 278 and 279, may be destroyed when three (3) years old or when all administrative needs have been met, whichever is later. Prior to destruction, Zero "0" file material must be reviewed and any policy material identified transferred to the corresponding Double Zero "00" file for permanent retention.

(7) Nontax Criminal Information: Destroy when five (5) years old, copies of correspondence maintained in administrative control files concerning nontax criminal information requested and obtained from the Internal Revenue Service (IRS).

(8) Freedom of Information and Privacy Acts Requests:

(a) Files containing correspondence and supporting documents (excluding official file copy of material if filed therein) TWO (2) YEARS after the date of reply, provided access was granted to all records requested and no appeal was filed; files containing responses to requester for nonexistent records, responses to requester who provided inadequate description, or those where requester failed to pay reproduction fees.

(b) Files and records relating to FOI/PA requests are authorized for destruction SIX (6) YEARS after the date of last relevant entry, reply to requester, final adjudication by court and/or FBI agreement to amend:

1. Records involved in litigation;

2. Those under appeal;

3. Those records involved in request to amend and/or expunge certain information;

4. Those files where access to all or part of the records requested was denied; and

5. Control file (Classification 190 only) for information disseminated to individuals and/or other agencies. (See MIOG, Part 1, 190-3.3(1).)

(9) Deleted

(10) Deleted

(11) Classification 116: LEAD OFFICE (FBIHQ is origin) case files in classification 116 created between November, 1947, and September, 1948, and contain no correspondence between the field office and FBIHQ are permanent and must be retained for eventual transfer to the NARA. Remaining lead office case files in the 116 classification may be destroyed if closed for twenty (20) years and none of the foregoing restrictions are applicable.

(12) Deleted

(13) Legat Files and Records:

(a) The NARA has designated all Hong Kong and Mexico City Legat investigative case files and corresponding index cards as exceptional/permanent; consequently, there will be no destruction of these records. All other Legat files and corresponding index cards are eligible for destruction when five (5) years old after application of the criteria of THE PLAN to identify exceptional/permanent case files in this collection. Closed Legat files are stored at FBIHQ; therefore, they will be reviewed by the Information Resources Division to identify and mark for preservation any exceptional/permanent Legat files. A numerical list of files to be transferred to the NARA and an alphabetical listing, by file number, of information indexed in exceptional/permanent Legat files will be furnished to all Legats with instructions to purge the Legat indices and forward the index records to FBIHQ to be matched with the corresponding exceptional/permanent file for eventual transfer to the NARA. After the index records have been purged and forwarded to FBIHQ, the

index purge list may be destroyed by the Legat. The numerical list of files transferred to the NARA should be retained by the Legat for future reference.

(b) Remaining Legat files, except Hong Kong and Mexico City, will be destroyed according to the five (5) year authority granted by the NARA. In conjunction with the destruction process, the files will be reviewed and a list made of all information indexed by Legats. The Legats, except Hong Kong and Mexico City, will be furnished a list of all files destroyed and a listing of all information indexed by the Legats. These listings are to be used by the Legats to purge and destroy the corresponding microfiche and index records. The list of information indexed may be destroyed once the index purge and destruction process have been completed. The list of files destroyed is to be retained by the Legat for future reference.

(14) Destruction of Original Foreign Intelligence/Foreign Counterintelligence (FCI) Electronic Surveillance Tape Recordings:

See Foreign Counterintelligence Manual (FCIM), Introduction, Section 1.

(15) Classification 67: FBI employment application case files pertaining to unsuccessful applicants, declined offers (by applicants) for employment and related correspondence which are maintained within classification 67 case files or control files in the various FBI field offices. Material maintained by field offices is duplicative of material maintained at FBIHQ inasmuch as FBIHQ is the office of origin and field offices are lead offices in classification 67 matters.

(a) Case files or control files wherein no appeal and/or litigation has been filed. Destroy when two years old or when all administrative needs have been met, whichever is later.

(b) Case files or control files wherein an appeal and/or litigation has been filed and which contain complaints with related correspondence, reports, exhibits, withdrawal notices, copies of decisions, records of hearings and meetings, and other records as described in Title 29, Code of Federal Regulations, Part 1613, Section 222 and resolved within the FBI, by Equal Employment Opportunity Commission or by United States Court(s). Destroy four years after final resolution of the case or when all administrative needs have been met, whichever is later.

(c) Field office case files or control files containing only correspondence and/or leads received from other field offices or FBIHQ which supplements the full background investigation which is being conducted primarily by FBIHQ or another field office. Destroy when six months old or when all administrative needs have been met, whichever is later.

(16) Contract Files:

Field office files which pertain to contracts, requisitions, purchase orders, leases, and bond and surety records, including correspondence and related papers pertaining to award, administration, receipt, inspection and payment of transactions. Destroy in accordance with Federal Acquisition Regulations Subpart 4.805, captioned "Storage, Handling and Disposal of Contract Files." Questions concerning these regulations should be directed to the Chief Contract Officer, Finance Division, FBIHQ.

(17) Contract Appeals Files:

Field office files which pertain to contract appeals case files arising under the Contracts Dispute Act, consisting of notices of appeal and acknowledgments thereof; correspondence between parties; copies of contracts, plans, specifications, exhibits, change orders, and amendments; transcripts of hearings; documents received from parties concerned; final decisions; and all other related papers. Destroy in accordance with Federal Acquisition Regulations Subpart 4.805, captioned "Storage, Handling and Disposal of Contract Files." Questions concerning these regulations should be directed to the Chief Contract Officer, Finance Division, FBIHQ.

2-4.5.3 Destruction - Noninvestigative Files and Records (See MAOP, Part 2, 2-4.3.1 (3)(h).)

(1) Classification 66 - Administrative case files accumulated by individual field offices containing material that relates to the internal administration or housekeeping activities of the office rather than the investigatory functions for which the office exists. In the absence of specific instructions set forth elsewhere in this manual, administrative material may be destroyed when one year old on an annual basis, except for the following administrative case files which must be retained for eventual transfer to the National Archives and Records Administration.

(a) "00" - Policy File

(b) Films

(c) Jails

(d) Sources of Information

(e) Surveillance

(f) Technical Equipment

(g) Technical Plants

(h) Technical Surveillance

(i) Microphone Surveillance

(j) Security Policy File

(k) Physical Security Of Building

(l) Security of Communications

(m) SAC Confidential Fund

(n) Persons Not To Be Contacted

(o) Congressional Committees

(p) Employee Services

(q) Detention And Security Index Program

(r) Arraignments

(s) Arrests

(t) Interviews including confessions and signed statements

(u) Searches and Seizures

(2) Copy Destruction

See MAOP, Part 2, 2-4.5.2 (2).

2-4.5.4 Destruction - Office of Origin Files and Records

(1) Office of origin case files in following case file classifications may be destroyed when 10 years old if none of the foregoing restrictions are applicable:

11, 13, 16, 18, 20, 22, 24, 30, 33, 34, 53, 57, 59, 68, 78, 84, 85, 95, 107, 135, 136, 154, 155, 169, 171

(2) Office of origin case files in following case file classifications, with less than two volumes (or number of serials as indicated) may be destroyed when 10 years old if none of the foregoing restrictions are applicable:

12, 28, 46, 54, 89, 147, 156, 159, 172, 177, 179, 183 (30 serials or less), 188 (10 serials or less), 192 (50 serials or less), 193, 194, 196, 205 (20 serials or less), 207, 208, 213 (45 serials or less), 245, 250 (25 serials or less), 252 (10 serials or less), 255 (75 serials or less), 262 (14 serials or less), 264 (25 serials or less), 265 (30 serials or less), 266 (30 serials or less)

(3) Office of origin case files in following classifications, with less than two volumes (or number of serials as indicated) may be destroyed when 20 years old if none of the foregoing restrictions are applicable:

1, 2 (40 serials or less), 3 (Exceptions: WF 3-4; WF 3-5 and NY 3-13), 14, 19, 39 (Opened prior to 1/1/78), 64, 97 (30 serials or less), 106, 117, 122 (11 serials or less), 173, 175 (8 serials or less), 191, 199 (20 serials or less), 201 (15 serials or less), 203 (15 serials or less), 215 (15 serials or less), 216 (15 serials or less), 217 (15 serials or less), 218 (15 serials or less), 219 (15 serials or less), 220 (15 serials or less), 221 (15 serials or less), 222 (15 serials or less), 223 (15 serials or less), 224 (15 serials or less), 225 (15 serials or less), 226 (15 serials or less), 227 (15 serials or less), 228 (15 serials or less), 229 (20 serials or less), 246 (15 serials or less), 247 (15 serials or less), and 248 (15 serials or less)

2-4.5.5 Destruction - Lead Office Files and Records

(1) Lead office case files in the following classifications may be destroyed one (1) year from the date of the last relevant communication, AND AFTER OBSERVANCE OF THE FOREGOING RESTRICTIONS/INSTRUCTIONS:

Classifications:

1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 64, 65, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 93, 95, 96, 97, 98, 99, 100, 102, 103, 104, 105, 106, 107, 108, 110, 111, 112, 113, 114, 115, 117, 118, 119, 120, 121, 122, 123, 124, 125, 126, 127, 128, 129, 130, 131, 132, 133, 136, 138, 139, 140,

141, 142, 143, 144, 145, 146, 147, 148, 149, 152, 153, 154, 155, 156, 157, 158, 159, 160, 161, 162, 163, 164, 165, 166, 167, 168, 169, 171, 172, 173, 174, 175, 176, 177, 178, 179, 180, 181, 182, 183, 184, 185, 186, 187, 188, 191, 192, 193, 194, 195, 196, 197, 198, 199, 200, 201, 202, 203, 204, 205, 206, 207, 208, 209, 210, 213, 214, 215, 216, 217, 218, 219, 220, 221, 222, 223, 224, 225, 226, 227, 228, 229, 230, 231, 232, 233, 234, 235, 236, 237, 238, 239, 240, 241, 242, 244, 245, 246, 247, 248, 249, 250, 251, 252, 253, 255 256, 257, 258, 259, 260, 262, 264, 265, and 266.

(2) DELETED.

(3) Classification 81

After a determination has been made that none of the foregoing restrictions are applicable, lead offices case files in classification 81 may be destroyed after one (1) year in all offices EXCEPT PORTLAND AND FORMER BUTTE FIELD OFFICE. BUTTE LEAD OFFICE FILES IN THE 81 CLASSIFICATION CREATED PRIOR TO THE BUTTE/SALT LAKE CITY MERGER June 6, 1989, AND NOW RESIDENT IN SALT LAKE CITY, ARE PERMANENT AND MUST BE RETAINED.

2-4.5.6 Deleted

2-4.5.7 Deleted

2-4.5.8 Deleted

2-4.5.9 Noninvestigative Files and Records to be Destroyed If More Than Six (6) Years and Three (3) Months Old

(1) Voucher Matters - Field office files containing voucher records processed as Direct Advance Vouchers or through the Third Party Draft System including, but not limited to, supporting documents, such as Draft Request Forms (FD-794), receipts, cancelled checks, bank statements, check stubs, and bank passbooks.

(2) Imprest Fund Matters - Field office files containing records processed for payment through the field office imprest fund.

2-4.5.10 Files and Records to be Destroyed If More Than Six (6) Years Old

(1) Automobiles - Accidents - Destroy six years after case is closed. Retain if loss of life, personal injury to third party, or possible suits involved.

(2) Health Record Cards - Cards containing dates of employees' visits, diagnosis, and treatment. Destroy six years after date of last entry on card.

(3) Time and Attendance Registers, FD-420 and FD-31 (obsolete) and Time and Attendance/TURK Registers, FD-420a (See MAOP, Part 2, 3-3.2.)

(4) All Leave Accounting Listings. Destroy when six years old, at end of leave year, or when administrative needs have been met, whichever is later.

(5) Leave Requests, FD-282

(6) Compensatory Time Request, FD-813

(7) Doctors' Certificates

(8) Confidential Financial Disclosure Reports (OGE-450) and Conflict of Interest Certifications (See MAOP, Part 1, 1-14 (14).)

(9) Bills of Lading

(10) Government Transportation Requests and related correspondence

(11) Household Goods - Transportation

(12) Correspondence relating to reimbursing individuals, such as travel orders, per diem vouchers, and all other supporting documents relating to official travel by officers, employees, dependents, or others authorized by law to travel.

(13) Lost or damaged shipment files - Schedules of valuables shipped and related correspondence.

2-4.5.11 Files and Records to be Destroyed When Five (5) Years Old, or Five (5) Years From the Date of Receipt or Disclosure, Whichever Is Longer

(1) Documents identified as tax returns and/or containing tax return information maintained in the field office (Classification 66) administrative control file entitled "Tax Return/Tax Return Information" may be destroyed five years from the date of receipt of the Internal Revenue Service (IRS) material or five years from the date of any disclosure, whichever is longer.

(2) General Training/Police Training/Firearms Training Matters - Field office administrative case files containing inquiries, requests, schedules, authorizations, and approvals for short-term training sessions(s) at the FBI Academy or within the immediate territory of a specific FBI field office. Material within the case files is utilized for individual registration, applicant scheduling and attendance purposes only. Case files serve no useful purpose to the field office after completion of the training session(s). Destroy when five years old or when all administrative needs have been met, whichever is later. Prior to destruction, all volumes will be screened by the FBI in order that any personnel-related material may be filed within the Official Personnel File (OPF) of FBI personnel or within the individual file of an FBI National Academy graduate. (See MAOP, Part II, 8-3.5.)

2-4.5.12 Files and Records to be Destroyed If More Than Three (3) Years Old (See MAOP, Part 2, 2-4.2.1.)

(1) Automobiles - After vehicle leaves custody by sale, transfer, donation, or exchange.

(2) Deleted

(3) Deleted

(4) Deleted

(5) Deleted

(6) Deleted

(7) Deleted

(8) Deleted

(9) Correspondence relating to position classification appeals. Destroy three years after resolution.

(10) Correspondence relating to employee appeals of performance ratings. Destroy three years after resolution.

(11) Tax Exemption Files - Tax exemption certificates and related papers. [redacted] Destroy three years after period covered by related account. b2

(12) Telephone Toll Statements, invoices, and toll slips (See MAOP, Part 2, 6-9.2.7.)

(13) Report of Excess Personal Property, SF-120

(14) Correspondence, reports, and data relating to voucher preparation

(15) Deleted

(16) Charity campaigns

(17) Deleted

(18) Deleted

(19) Deleted

(20) Deleted

(21) Deleted

(22) Semiannual Motor Vehicle Report, FD-111

(23) Radio Equipment Maintenance Log, FD-341. Retain for three years after completion.

(24) Postal Irregularities - Correspondence relating to irregularities in the handling of mail, such as loss or shortage of postage stamps or money orders or loss or destruction of mail. Destroy three years after investigation completed.

(25) Printing and duplicating - Files and correspondence pertaining to planning and other technical matters relating to the printing and duplicating function.

(26) Telecommunications general files, including plans, reports, and other records pertaining to equipment requests, telephone service and similar matters.

(27) Speech material - except one copy of speech material of continuing interest.

(28) Quarterly and/or semiannual reports of the national organization of the Communist Party USA, furnished all offices by New York. If desired, individual offices may maintain for historical value. New York will retain.

(29) Copies of annual, semiannual, or quarterly letters or reports submitted concerning informants (FD-374) or confidential witnesses and data maintained in field office control file.

(30) Firearms

(31) Inspections (For destruction of work papers, see MAOP, Part 2, 2-4.5.13(7).)

(32) Office Personnel File (SAC is to review prior to destruction and specify documents to be retained longer than three years.) (See MAOP, Part 2, 2-4.5.17(2).)

(33) Memorandum to All SACs (formerly SAC Letters), and Bureau bulletins. Carefully review to ensure that instructions which are still applicable and which will be of future value are not destroyed prematurely. (See MAOP, Part 2, 2-4.2.1(3) & 2-4.5.17(4).)

(34) Monthly Administrative Reports, FD-29 and FD-29a

(35) Foreign National Field Office Control Files - Records pertaining to the movement of foreign nationals to and from the United States. Control files only; field office investigative case files are to be retained/destroyed commensurate with the disposition authority applicable to the specific case file classification wherein the material is maintained.

(36) Equal Employment Opportunity (EEO) Control Files - General correspondence, copies of regulations with related records pertaining to the Civil Rights Act of 1964, the EEO Act of 1972, any pertinent later legislation and EEO Committee meeting records (including minutes and reports)

(37) Deleted

(38) Voucher Matters - Field office files containing voucher records which have been forwarded to FBIHQ for payment.

(39) Restoration of Annual Leave Requests - Standard Form (SF) 71 or equivalent and all supporting documentation of requests and approvals of restoration of annual leave. Destroy three years after end of leave year during which annual leave was originally earned.

2-4.5.13 Files and Records to be Destroyed When Two Years Old or After Office Inspection, Whichever Is Later (See MAOP, Part 2, 2-4.2.1.)

(1) Daily Reports, FD-28

(2) Record of Agents' individual accomplishments

(3) Copies of correspondence requesting record checks of [redacted] and Passport Office, Department of State, maintained in control file. b2

(4) Deleted

(5) Deleted

(6) Deleted

(7) Inspection work papers (yellows) covering prior inspection provided inspection just completed was full inspection and not a recheck. If longer retention deemed essential, appropriate notation to be made. (See Part 2, 2-4.5.12(31).)

(8) Copies of the Accomplishment Report (FD-515) maintained in the control file.

(9) Authorization to maintain Bureau Vehicle Overnight at Agent's Residence on Irregular and/or Emergency Basis, FD-490.

(10) Original Agent File Review Sheets (FD-271) maintained for inspection purposes.

(11) Pending Transcription Workload and Delinquency Report (FD-703) and Automated Workload Tracking Reports.

(12) FD-515 Cumulative/Comparative Reports - Field office control file containing summary of statistical accomplishments accumulated from FD-515 by individual program(s).

(13) Resource Management Information System - Field office control files (including subfiles) containing resource management statistical information, i.e., manpower allotment, manpower hours utilized, individual program(s) accomplishments and projections.

(14) Unaddressed Work - Field office control files containing correspondence and/or leads which, prior to the implementation of the Automated Case Support (ACS) system, were unaddressed and are currently in ACS as closed case files. (See MAOP, Part 2, Section 2-5.2.5.)

2-4.5.14 Deleted

2-4.5.15 Files and Records to be Destroyed When Two Years Old, If Certain Conditions Are Met (See MAOP, Part 2, 2-4.2.1.)

(1) Deleted

(2) Supply Management Matters - Files containing original correspondence relating to supply requirements and procurement matter submitted for internal supply management operation and administration, exclusive of that original material which has been incorporated into investigative case files, or that material which has been forwarded to FBIHQ.

(3) Ammunition - Destroy two years after completion or cancellation of requisition.

(4) Inventory/Requisition Matters - General files containing requisitions, inventory lists and inventory cards for supplies and equipment necessary to supplement and/or maintain current inventory, exclusive of that material which has been incorporated into specific investigative case files, or that material which has been forwarded to FBIHQ.

(5) Property Disposal Correspondence Files - Correspondence maintained by units responsible for property disposal, pertaining to their operation and administration.

(6) Space files and related correspondence pertaining to the allocation, use, and release of space under agency and/or General Services Administration (GSA) control. Destroy two years after termination of space assignment, when lease is canceled, or when plans are superseded or obsolete.

(7) Files and correspondence relating to the administration, operation, and execution of the copying, duplicating, and printing functions.

(8) Procurement matters - ORIGINAL correspondence files concerning internal operation and administration not forwarded to FBIHQ.

(9) Deleted

(10) Equal Employment Opportunity (EEO) Counselors' notes. Destroy two years after the date of creation, unless the EEO Counselor forwards them to FBIHQ for storage and later destruction (see MAOP, Part 1, 4-5.1.4 and 4-5.1.5).

(11) Deleted

(12) Complaint Form (FD-71) - Control Files only; field office investigative case files opened as a result of information recorded on FD-71 are to be retained/destroyed commensurate with the disposition authority applicable to the specific case file wherein the material is maintained.

(13) Administrative case files containing correspondence, memoranda, annuity estimates, and other records used to assist retiring employees or survivors claim insurance or retirement benefits, including but not limited to reports, registers, or other control documents, and other records relating to retirement, such as SF-2807 or equivalent.

(14) United States Postal Service (USPS) records and mail and delivery service control files - Including record of Registered Mail FD-211; USPS Forms 3877 (outgoing registered mail) and 3883 (incoming registered mail); records relating to certified, insured, and special delivery mail, including receipts and return receipts; application for USPS registration and certificates of declared value of matter subject to USPS surcharge; reports of loss, rifling, delay, and other improper treatment of mail matter; records of receipt and routing of incoming and outgoing mail and items handled by private delivery companies, i.e., Federal Express (FedEx), United Parcel Service (UPS), DHL, etc.; statistical reports on mail handled and work performed; records relating to checks, cash, stamps, money orders, or other valuables remitted by mail; and correspondence relating to the administration of the mail room operation. (See also MAOP, Part 2, 2-2.1 and 2-2.2.2.)

2-4.5.16 Files and Records to be Destroyed When One Year Old, If Certain Conditions Are Met

(1) Deleted

(2) Copies of correspondence forwarded to Office of Personnel Management relating to performance rating board reviews. Destroy one year after case is resolved (for files created prior to the Civil Service Reform Act of 1978).

(3) Notice of Tardiness, FD-120. Destroy when one year old at the end of the calendar year.

(4) Deleted

(5) Deleted

(6) Deleted

(7) Forms

(8) Gun Vault Charge-Out Records, FD-79

(9) Bank robbery, bank burglary, and bank larceny summaries

(10) Theft from Interstate Shipment and Interstate Transportation of Stolen Property summaries

(11) New Agents' Training Unit class books.

(12) Voluntary Leave Transfer Program Records - Administrative case files documenting the receipt and donation of leave for medical emergencies, including receipt applications, FBIHQ/field office approvals or denials, medical or physician certifications, leave donation records or OF-630-A,

supervisor/timekeeper approvals, leave transfer records, payroll notification records, and leave program termination records.

(13) Form FD-430 (Bank Robbery Statistical Airtel) - Field Control File copy only.

(14) Fugitive Bank Robbery (FUBANK) circulars - Field Control File copy only.

(15) National Bank Robbery Album (NABRA) circulars - Field Control File copy only.

2-4.5.17 Files and Records to be Destroyed When One Year Old on an Annual Basis

(1) Deleted

(2) Office Personnel File - Destroy obsolete temporary documents relating to Bureau personnel only. (See Part 2, 2-4.5.12 (32), for disposition of remaining documents.)

(3) Firearms Score Card, FD-39

(4) Memoranda to All Special Agents in Charge (formerly SAC Letters) - Review prior to destruction in order to identify and retain any policy and/or instructions which is still applicable. (See MAOP, Part 2, 2-4.2.1 (3) and 2-4.5.12 (33).)

(5) Individual Security Patrol Daily Report, FD-215; Combined Security Patrol Report, FD-215a; and Security Patrol Log, FD-215b.

(6) Security and Complaint Assistant Daily Report Sheet (FD-694).

(7) Volumes of letters, often from chronic letter writers, which do not require acknowledgment. Correspondence is nonspecific, frequently incoherent, and contains no data of interest to the FBI or any other agency.

2-4.5.18 Files and Records to be Destroyed When One Year Old on a Monthly Basis

(1) Deleted

(2) Except New York and Washington Field Offices: Copies of INS form I-94 or equivalent form used locally to furnish information from the I-94 to FBIHQ which pertain to individuals within the provisions of the National Foreign Intelligence Program Manual, and which are retained in control files only and the index cards relating thereto.

2-4.5.19 Files and Records to be Destroyed When Six Months Old, If Certain Conditions are Met

(1) Deleted

(2) Field Stenographer's and Typist's Daily Report, FD-76

(3) HF Radio Log, FD-279

(4) Telecommunications message registers, logs, performance reports, daily load reports, and related and similar records.

2-4.5.20 Files and Records to be Destroyed When Four Months Old, If Certain Conditions Are Met

(1) Field Personnel Files - Files of employees who have retired, resigned, or transferred to other agencies outside of the FBI. Material maintained by field offices is duplicative of material maintained at FBIHQ inasmuch as FBIHQ is the office of origin and field offices are lead offices in classification 67 matters.

(a) Case files wherein no appeal, litigation grievance, lawsuit or any kind of employment related complaint, has been filed. Retain for a period of 120 days after retirement, resignation, or transfer of employee; then destroy.

(b) Case files wherein an appeal, litigation grievance, lawsuit or any kind of employment related complaint, has been filed. Forward file to FBIHQ along with an explanation of the circumstances requiring retention of the file. A copy of the explanation must be provided to the Office of the General Counsel, Employment Law Unit (ELU). FBIHQ will file the Field Personnel File with the FBIHQ Official Personnel Folder and retain the Field Personnel File until instructed to destroy it by the Office of the General Counsel, ELU.

2-4.5.21 Files and Records to be Destroyed When Three Months Old, If Certain Conditions Are Met

(1) Transmittal letters - checks and bonds

(2) Automobile Record Form, FD-73

(3) FM Radio Station Log, FD-283 (See MIOG, Part 2, 16-4.2.4.)

(4) Gasoline sales tickets (tissue copy)

(5) Deleted

(6) Identification credentials, including cards, badges, parking permits, photographs, agency permits to operate motor vehicles; property, dining room, and visitors' passes; and other identification credentials. Destroy three months after return. (See MAOP, Part 2, 6-10.2 (3).)

(7) Building and Equipment Service Files - Requests for building and equipment maintenance services, excluding fiscal copies. Destroy three months after work performed or requisition canceled.

(8) Carbon copy of printout produced by NCIC terminal not required to be retained. However, an NCIC log must be maintained for all criminal history record checks; the log will be maintained for a minimum of one year.

(9) Unless required as part of a review or investigation, alarm log sheets and paper tape records of all alarm calls received shall be destroyed when no longer required after three (3) months.

(10) Visiting employees log, FD-426

(11) Routine requests for information or publications and copies of replies which require no administrative action, no policy decision, and no special compilation or research for reply.

2-4.5.22 Files and Records to be Destroyed When Two Months Old, If Certain Conditions Are Met

(1) Messenger Service Files - Daily logs, assignment records and instructions, dispatch records, delivery receipts, route schedules, and similar records related to the messenger function.

(2) Telecommunications - Copies of incoming and outgoing messages retained in the message center.

2-4.5.23 Files and Records to be Destroyed When Purpose Has Been Served (See MAOP, Part 2, 2-4.2.1.)

(1) Request for Personnel Action, SF-52 (when used to advise of arrival date of a transferred employee into the field office)

(2) Itinerary, FD-330

(3) Circulars, flyers related to charity campaigns, recreational matters, open season for thrift savings program, open season for health/life insurance/retirement benefits, blood donor program, savings bond campaign.

(4) Copies of SF-50 documenting individual personnel actions.

(5) Credentials - Papers related to identification credentials, including receipts, indices, listings, and accountable records. Destroy when all listed credentials are accounted for.

(6) Telecommunications - Tapes of outgoing messages. Destroy after transmission.

(7) Channelizing memoranda in criminal cases and security cases must be destroyed following submission of reports or following submission of LHM in nonprosecutable espionage and nationalistic tendency cases.

(8) Channelizing memoranda in security cases must be destroyed when the contents have not been included in a report or LHM because the information is of no value to the report or LHM. In destroying these memoranda, be guided by the following instructions:

(a) The Agent, at the time he/she dictates the report or the LHM in nonprosecutable espionage and nationalistic tendency cases, is to prepare a memorandum (Form FD-338) listing the channelizing memoranda to be destroyed by serial or serial scope and requesting Administrative Officer to destroy. List channelizing memoranda to be destroyed because they are of no value to the report or LHM by file and serial number. This memorandum should indicate that pertinent information contained in the serials to be destroyed was incorporated in the report or the LHM, or in security cases was not included because the information was of no value to the report or LHM.

(b) The cover pages accompanying the report or the cover document accompanying the LHM will list the file and serial number of the original informant reports or master channelizing memoranda except in cases concerning reports or LHM prepared by Legal Attaches since Legat sources are not usually available for testimony.

(c) In the case of multiple volumes, the destruction memorandum should be prepared by the Agent in sufficient numbers so that one copy will appear in each volume of the multiple volume file being stripped.

(d) Prior to destruction, the Agent's recommendations are to be reviewed and approved by the supervisor at the time he/she reviews and approves the report or the LHM.

(e) Employee destroying the channelizing memoranda must place date of destruction and his/her initials on the destruction memorandum. Thereafter, this memorandum will be filed in the case as a permanent record of the serials destroyed.

(f) Channelizing memoranda based on confidential investigative techniques may be destroyed after submission of LHM or report. The cover pages of the report or the cover document of the LHM must record the exact location in the office files of the original information.

(g) Channelizing memoranda of translations of foreign language newspapers and periodicals may be destroyed provided the original translation is maintained in the main file of the publication concerned.

(h) Channelizing memoranda from other offices may be destroyed provided the communication of transmittal and one copy of the channelizing memoranda are retained in your office. The cover pages to the report or the cover document to the LHM should list field office and the file number in which the original recording is located, as well as location in your files of the retained copy.

(9) Do not destroy channelizing memoranda in the following instances: The original recording; serial one of a file regardless of its nature; serials containing indexing. It would appear that if indexing was necessary to channelizing memoranda, such indexing would only be done in the main case file as set forth in the title of the communication; serials showing "action" information: e.g., opening, closing, posting, or instructions given by a supervisor to an Agent concerning the case.

(10) The destruction of those channelizing memoranda should be subject to close supervisory control to ensure that all pertinent information contained in these memoranda is reported in the investigative report or the LHM.

(11) Stop notice cards and correspondence received by field offices requesting affirmative action in connection with stop notices placed with Immigration and Naturalization Service (INS) and Bureau of Prisons (BOP) maintained in administrative file (if no case file exists) when stop notices have been canceled or expire.

(12) Deleted

(13) Teletype summaries or reproduced copies of teletype summaries on civil unrest sent to all field offices by FBIHQ.

(14) Deleted

(15) Routing of Earnings and Leave Record, FD-655.

(16) Field Office Special Surveillance Group (SSG) Daily Worksheets - Control files which have been arranged in monthly volumes and workshift for the purpose of gathering and maintaining statistics used for administrative purposes.

(17) Weekly Press Summary File (WPSF)/National Periodical Summary File (NPSF) - Volumes of copies of newspaper articles from various national/international newspapers (WPSF) and periodicals (NPSF). Material is furnished to field offices and Legal Attaches by the Office of

Congressional and Public Affairs, FBIHQ, for informational/reference purposes ONLY. Retention by the field office or Legal Attaches is OPTIONAL.

(18) Investigator - Case files containing past issues of FBI employee magazine "The Investigator." Formal filing of "The Investigator" is unnecessary.

(19) Internal office memoranda unique to individual FBIHQ division, field office, resident agency or Legal Attache Office and accumulated solely for the internal administration of each individual entity.

(20) Dissemination Files - Field office control files containing correspondence and/or lead(s) received from other field offices. Leads are disseminated to appropriate field office squad, resident agency, or local law enforcement agency for follow-up. Material has been accumulated solely as a "tracking system" of official records disseminated to other agencies and filed for administrative purposes only inasmuch as lead(s) usually meet with negative results. Case files opened as a result of dissemination of correspondence and/or lead(s) are to be retained/destroyed commensurate with the disposition authority applicable to the specific case file wherein the material is maintained.

(21) Law Enforcement Bulletin and related Indexing Lists - Material is furnished to field offices and Legal Attaches for informational/reference purposes related to training activities. Official filing is NOT REQUIRED and any future retention, for reference purposes only, should be at the discretion of the field office Training Coordinator.

(23) FBI Recreation Association (FBIRA) - Administrative case files pertaining to the overall functions of the FBIRA. Formal filing of FBIRA material is unnecessary. Material pertinent to the organization and/or operation of the FBIRA should be put under the control of the field office FBIRA committee, as chosen by the field office employees.

(24) Terrorist Photograph Album - Terrorist Photograph Album has been discontinued and FD-432's and FD-432a forms are no longer to be maintained in an album (file) but serialized into the subject's substantive file or main organizational file.

(25) FBI Bomb Data Center Investigators Bulletins and Monthly Incident Summaries - Material is furnished to field offices and Legal Attaches for informational/reference purposes related to training activities. Official filing is NOT REQUIRED and any future retention, for reference purposes only, should be at the discretion of the field office Special Agent Bomb Technician or Training Coordinator.

(26) Routine communications from individual field offices to FBIHQ, field offices, resident agencies and Legal Attaches of routine advisement, i.e., telephone problems, death notices, promotion/transfer/reassignment notices, etc., which require no administrative action, policy decision, or reply. Material is furnished to various entities for informational and/or reference purposes only. Official filing is NOT REQUIRED.

(27) Notices of Vacancy - Copies of notices of vacancy, exclusive of official record copy maintained within position selection file. Filing of copies outside of official selection file is NOT REQUIRED. See MAOP, Part 1, 7-6.7 for contents and maintenance of official selection file.

2-4.5.24 Deleted

2-4.5.25 Records to be Destroyed After Separation or Transfer of Employee

Employee record cards used for informational purposes.

2-4.5.26 Files and Records to be Destroyed When Abolished or Superseded

(1) Copies of position descriptions and related correspondence

(2) Copies of official publications, charts, posters, directives, regulations, forms, press releases or similar material.

(3) Instructions from FBIHQ sent to all field offices, not filed within the appropriate Double Zero "00" case file. Prior to destruction, file material must be reviewed and any policy and/or instructions which is still applicable and not previously filed in appropriate Double Zero "00" case file transferred accordingly.

2-4.5.27 Files and Records to be Destroyed When Canceled or Revised

Mailing lists - Correspondence, request forms, and other records relating to changes in mailing lists and card lists. Destroy when canceled or revised, whichever is appropriate.

2-4.5.28 Files and Records to be Destroyed Upon Termination or Completion

(1) Copies of routine procurement files, including contract, requisition, purchase order, lease, and bond and surety records. (Excluding original correspondence not forwarded to FBIHQ)

(2) Copies of successful or unsuccessful bids.

2-4.5.29 Files To Be Destroyed Upon Notification From FBIHQ

(1) Office of Professional Responsibility (OPR) case files maintained by field offices may be destroyed upon receipt of notification from Administrative Summary Unit, Personnel Division, FBIHQ, that the OPR matter has been resolved.

(2) Case files which have been stamped with OCIS/ISIS/ISS/TIS notations. Destroy office of origin case files in accordance with destruction authority granted by FBIHQ. Auxiliary office case files may be destroyed after a determination has been made that none of the foregoing restrictions are applicable.

2-5 CASE MANAGEMENT - FIELD OFFICES

2-5.1 Opening Cases (See NFIP Manual, 19-03, M.)

(1) When one or more interviews are to be conducted

(2) When the USA is consulted and a written record of USA's opinion furnished USA

(3) When an informant is being operated.

(4) In considering the above it should be borne in mind when a file is opened designating a particular individual as the subject of that file that the Bureau be in the position to justify the

establishment and later the maintenance of that file on the grounds that there is sufficient jurisdiction for the Bureau to investigate that matter as a separate activity. This is also applicable to the use of subfiles, meaning that if such a file is opened it must meet this test.

(a) The universal list of subfiles, and the standard code assigned to each subfile are listed below. These subfiles should be used when appropriate. The subfiles are not to be opened until a specific need exists.

STANDARD SUBFILE: CODE:

1A Exhibits 1A FD-192s (Evidence) 1B FD-192As (Bulky, Nonevidence) 1C FD-302s and inserts 302 Background Information re subject BC (FD-160, FD-125, FD-809) Case Expenditures CE ELSUR Administrative (Criminal & FCI matters) ELA ELSUR Original Logs (Criminal and FCI) EL1 ELSUR Copies and Logs (Criminal and FCI) EL1A ELSUR Transcripts (Criminal and FCI) EL1B Grand Jury Material GJ Physical Surveillance Logs FISUR Forfeiture FF Lab/Latent Reports LAB Mail Covers MC Newspaper Clippings (Press Releases) NC Subpoenas SBP Telephone Subscriber and Telephone TEL Toll Information

(b) When more than one subfile is needed for a specific category, numbers are to be used following the code. For example, three Forfeiture subfiles would be named: FF1, FF2, FF3, etc.

(c) With regard to ELSUR usage in both criminal and FCI matters, subfiles will be opened for the purpose of maintaining the administrative correspondence relating to the ELSUR usage. Where more than one ELSUR authorization is sought/obtained, additional subfiles may be opened and named ELA2, ELA3, ELA4, etc. In each case a subfile for retaining original logs and hard copy printouts of communications intercepted in criminal and FCI matters will be opened and named EL1. Multiple installations in a given case will require additional subfiles, i.e., EL2, EL3, EL4, etc. COPIES of these logs/printouts are to be retained in a subfile named EL1A. Multiple installations will require additional subfiles for COPIES of these logs, i.e., EL2A, EL3A, EL4A, etc. Full text or partial transcripts of intercepts are to be maintained in subfiles named EL1B.

(d) The Manual of Investigative Operations and Guidelines (MIOG), Part 1, Section 137-15, sets forth policy for maintaining Criminal Informant (CI)/Cooperating Witness (CW) subfiles.

(e) The National Foreign Intelligence Program Manual, Section 27-25, sets forth policy for FCI and International Terrorism (IT) Assets subfiles.

(f) The MIOG, Part 2, 2-9.7, sets forth policy for grand jury material subfiles.

(5) The initials of a supervisor must be placed on the serial opening or reopening a case. In opening new fugitive cases each fugitive subject must be assigned a letter priority designation. The supervisor will make the appropriate letter designation on the lower left hand corner of the opening serial. (See MIOG, Part 2, 21-2.)

(6) Crime Problem Indicator (CPI) Codes:

(a) Definition and Use: CPI codes are mechanisms by which investigations can be "tagged" as pertinent to specific direct-funded initiatives and national crime problems, some of which require Congressional reporting on statistics, but which may span more than one investigative classification

or program. By reviewing the various crime problems encountered in cases, the FBI will be able to request funding commensurate with its needs.

(b) Assigning CPI Codes: The squad supervisor or Legat (whoever is approving the case opening) should indicate all applicable CPI codes for every new investigative case opened or reopened, along with the classification, case Agent, date opened, etc. The Information Management Assistant will designate the CPI codes in ACS in the Open and Assign Case section of the Case Management Menu, ICM. Up to 20 CPI codes may be identified per case. If no CPI codes apply, the "none" value must be entered.

(c) Reports: Reports to obtain statistical information regarding CPI codes may be run by FBIHQ from ACS or from the Integrated Statistical Reporting and Analysis Application (ISRAA).

2-5.1.1 Leads (See MAOP, Part 2, 10-16.15.)

(1) Leads are set to offices and assigned to individuals/organizations in order to aid in the investigation. When the OO sets a lead to another office, that office is considered a Lead Office.

(2) There are three types of leads: Action Required, Discretionary Action, and Information Only.

(a) Action Required leads are used if the sending office requires the receiving office to take some type of action. Action Required leads cannot be set out of zero (0) and double zero (00) files.

(b) Discretionary Action leads are used if the sending office has some information that may be of importance to the receiving office. These leads may or may not require action by the recipient, and the recipient will decide what, if any, action to take. Discretionary Action leads can be set out of zero (0) and double zero (00) files.

(c) Information Only leads are used for information only and when no specific action is required or necessary. Information Only leads can be set out of zero (0) and double zero (00) files.

(3) Leads are covered once the investigation or request has been completed. Discretionary Action and Information Only leads can be covered while they are in the "Set" status. These leads do not have to be assigned in order to be covered.

2-5.2 Status of Cases

(1) The status of the case shall be marked on the top cover of a file in the lower right corner as follows:

(a) Deleted

(b) Assigned - All active investigative cases must be assigned immediately upon receipt. Name of employee or squad/unit to whom assigned and date must be entered.

(c) Closed - C and date

(d) Deleted

(e) Deleted

(f) Pending inactive - P*

(g) Deleted

(2) When the status of a case is changed, the top cover should be marked accordingly.

2-5.2.1 Pending Case

A case is pending when there is work remaining to be done or to be reported.

Every 90 days, the Administrative Officer (AO)/Office Services Manager (OSM) or Legat is required to print the PENDING CASES report from ACS. This report is to be balanced against the actual pending cases in the office. The reports, with appropriate verification markings, should be filed in the same file containing the copy of the Monthly Administrative Report.

2-5.2.2 Pending Inactive

(1) Instructions to the Administrative Officer (AO)/Office Services Manager (OSM) to place a case in pending-inactive status must be in writing on the appropriate serial, which must be initialed and dated by the supervisory employee and flagged for the AO's/OSM's attention.

(2) A case should be placed in a pending-inactive status when:

(a) All investigation has been completed and only prosecutive action or other disposition remains to be determined and reported;

(b) Deleted

(c) In fugitive cases, refer to the "Pending Inactive Status when all Logical Investigation has been Conducted," and "Locating and Relocating Fugitives Outside the United States" citations appearing in MIOG, "Fugitive-General" Section, Part 2, Section 21.

(3) Pending-inactive cases can be assigned to investigative personnel or a squad/unit.

2-5.2.3 Referred Upon Completion to the Office of Origin (RUC)

The status of RUC was eliminated with the implementation of the Automated Case Support (ACS) system. RUC was used when an auxiliary office had completed their investigation, i.e., covered all of their leads. Auxiliary offices were renamed Lead Offices upon the implementation of ACS and no longer opened new cases in existing matters, but worked leads off of the OO's case; therefore, the status of RUC was no longer needed.

2-5.2.4 Closed (See MAOP, Part 2, 3-4.5 (9) (d).)

(1) Case may be closed when:

(a) The USA declines prosecution

(b) The federal grand jury returns a "No Bill"

(c) A nolle prosequi has been entered

(d) Final prosecutive action has been completed

(e) All leads have been exhausted and the SAC authorizes closing. SAC's opinion must be based on the belief that further investigation would not be warranted

(f) In antitrust cases, the original complaint is received

(g) In a Lobbying Act case, the original complaint is received

(h) In routine deserter cases, a communication is received from the apprehending office; in nonroutine deserter cases, a communication is received from apprehending field office (See MIOG, Part 1, 42-6 and 42-12.)

(i) In parole, mandatory release, and probation violator cases, a report, teletype, or electronic communication (EC) is received from apprehending field office

(j) In bank robbery statute violations, in selective instances by EC (See MIOG, Part 1, Section 91.)

(k) In involuntary servitude and slavery cases, an initial investigation has been conducted, and all logical leads have been exhausted

(l) In civil rights cases involving allegations of police brutality, the initial investigation has been conducted pursuant to MIOG, Part 1, Section 282-4.1 and, in the opinion of the SAC, the totality of the circumstances indicates that the case is not of a serious or substantial nature and does not warrant further investigation. In all other civil rights cases, when logical investigation has been conducted (See MIOG, Part 1, 50-4 (1).)

(m) Deleted

(n) In election laws cases, the original complaint is received

(o) In cases under Civil Rights Act of 1964, when preliminary or limited investigation has been conducted

(p) In antiriot laws cases, a preliminary investigation has been conducted

(q) In discrimination in housing cases, an initial investigation has been conducted, and all logical leads have been exhausted

(r) Deleted

(2) Bankruptcy cases must be presented to USA and cannot be closed administratively. (See MIOG, Part 1, 49-5.)

(3) The initials of a supervisor must be placed on the serial closing a case administratively.

(4) When a case is closed, the office of origin must, by teletype or EC, immediately advise lead offices.

(5) When office of origin or lead office obtains information which would seem to preclude any further investigation of a case or of any phase of it, appropriate offices and FBIHQ should be advised immediately. If there is nothing additional to be done by receiving offices, they may close administratively (except full-field public corruption investigations, which only may be closed by declination). This instruction includes office of origin if status report only would have been submitted. (See MAOP, Part 2, 10-9 (10); MIOG, Part 1, 58-6.7, 58-8.4, 194-5.7 and 194-8.4.)

(6) Ten Most Wanted Fugitive cases, after being so designated, must be kept pending in all field offices until a complete review of the case has been made and all logical investigation has been conducted.

2-5.2.5 Unaddressed Work (UNAD) (See MAOP, Part 2, 2-4.5.13.)

(1) UNAD is defined as investigative matters that cannot be adequately addressed by available manpower. These investigative matters could be either new cases in an office or pending cases which cannot be handled at the current time due to a shift of manpower priorities.

(a) Allegations of criminal activity which are not within the prosecutive guidelines of each office and, as a result, subject to blanket declinations, should not be recorded as UNAD. Each of the sections relating to the FBI investigative classifications in the MIOG should be reviewed to determine if policy and procedures for the classification would prohibit utilizing UNAD status.

(b) Each SAC must ensure that: (1) all available investigative resources are being fully utilized on investigative matters prior to recording allegations and/or events as UNAD and (2) a periodic review of these matters must be conducted by the Supervisory Special Agents (SSA) and the Supervisory Senior Resident Agents (SSRA).

(c) Allegation or events which are recorded as UNAD must be periodically reviewed to determine whether there is any concurrent federal, state or local investigative jurisdiction. If concurrent jurisdiction exists, the matter must be referred in writing to the appropriate law enforcement agency within 30 days of making the case UNAD.

(2) UNAD matters can be placed in a UNAD Control File, and a periodic review of this file must be conducted by the SSA and the SSRA. See MAOP, Part 2, Section 2-4.1.5 for the existing policy pertaining to Control Files.

(3) At the discretion of each office and/or SSA, UNAD matters can be opened and assigned a Universal Case File Number (UCFN) through the Investigative Case Management application of the Automated Case Support (ACS) system.

(a) Deleted

(b) Deleted

(c) Deleted

(d) Deleted

(e) For new cases, the Information Management Analyst/Clerk (IMA/IMC) will open the case with a case type of "U," status of "P" for pending, and assign it to the appropriate squad. The IMA/IMC opens the case through the Investigative Case Management application of ACS.

(f) The matter will be assigned a UCFN, but will not be counted or reflected on the Monthly Administrative Report (MAR). The physical filing methodology and storage of these UNAD matters is left to the discretion of each field office. The decisions made, however, should be documented and indexed under UNAD to an appropriate administrative/control file within each office for subsequent compliance review.

(g) For existing pending cases, the IMA/IMC will close the case administratively (C4) (all leads are covered or discontinued). Then the case is reopened as a UNAD case, with a case type of "U."

(h) A report for all UNAD cases is available in the automated environment. This report is called the CASE TYPE REPORT (the Case Type is "U") and is located in the Case Reports Menu of ICM, ACS. Upon request of the SSA or SSRA, the IMA/IMC can close UNAD cases by changing the status to C4 or C6.

(i) Upon request of the SSA or SSRA, the IMA/IMC can change a UNAD cases to a pending investigative case. The IMA/IMC will close the UNAD case administratively (C4) and reopen the case without a case type (blank = investigative.

2-5.3 Tickler Application

(1) Tickler Application

The Tickler Application in the Automated Case Support (ACS) system can be used to follow and track cases/leads.

(2) Deleted

(a) Deleted

(b) Deleted

(c) Deleted

(d) Deleted

(3) Deleted

2-5.3.1 Deleted

2-5.3.2 Deleted

2-5.3.3 Deleted

2-5.3.4 Deleted

2-5.3.5 Deleted

2-5.3.6 Deleted

2-5.3.7 Deleted

2-5.3.8 Deleted

2-5.3.9 Deleted

2-5.4 Reports

2-5.4.1 Deleted

2-5.4.2 Daily Report of Security Patrol Clerk (FD-215)

The daily report of the Security Patrol Clerk is a white form made up so that the date, name of employee, hours worked, name of building, time, area covered, remarks, security of Bureau automobiles, security of Bureau automobile keys (if applicable), including time and remarks, and signature can be entered. The security patrol clerk must submit this form daily to the SAC for review and approval. In those field offices and FBIHQ divisions where Security Patrol Clerks are supervised directly by an SA, they will not be required to execute Form FD-215. Form FD-215a (Combined Security Patrol Report) will continue to be used.

2-5.4.3 Deleted

2-6 ACCOUNTING INVESTIGATIONS

Set forth below are the types of cases which the Bureau considers to be actual accounting cases and accounting-type cases. This list is to be used as a guide in determining whether an investigation falls within the category of an accounting matter.

2-6.1 Actual Accounting Cases

(1) Where the investigation actually entails the detailed examination of books and records.

(2) Where there is a possibility that testimony may be required as to accounting matters.

These cases are to be assigned to a Special Agent Accountant (SAA) in every instance.

2-6.2 Accounting-Type Cases

(1) Those cases in which, although no detailed examination of books and records is required, the investigation entails the tracing of billings from one company to another or to the U.S. Government. This situation occurs in many fraud against the Government cases.

(2) Those cases in which the matter can be handled more effectively by an SAA since the investigation involves the review and interpretation of financial statements, bank records, and similar data with which an accountant is more familiar. One example of this situation is a lead in a bankruptcy case to interview customers of the bankrupt where such interviews necessarily require an inspection of accounts payable records and supporting data.

(3) Those cases requiring an interview or series of interviews dealing with business administration or operations which because of accountant's educational background and previous experience an accountant may be more qualified to handle.

(4) These cases should be assigned to an SAA when an accountant is available. These cases may be assigned to nonaccountants where it appears a nonaccountant is capable of handling the matter properly and an accountant is not available.

2-6.3 Policy

(1) The SAC, ASAC, and field supervisors will be held personally responsible to ensure that SAAs are assigned to matters where their accounting background and training can be utilized effectively when such matters are pending in a field office.

(2) When an SAA has developed to the extent where SAA has additional qualifications over those previously reported, inform FBIHQ by letter for the attention of the Criminal Investigative Division.